CRISTIAN
TRONCOTĂ
Coordonator

STUDII DE
TRITONIC
SECURITATE

Neliniștile Insecurității

NELINIȘTILE INSECURITĂȚII

© COPYRIGHT TRITONIC
BUCUREŞTI / ROMÂNIA 2005
e-mail: editura@tritonic.ro
tel./fax.: +40.21.242.54.09

www.jurnalism.ro
www.tritonic.ro
www.studiidesecuritate.ro

Colecţia: STUDII DE SECURITATE
Coordonator: MIREILLE RĂDOI

La realizarea acestui volum au participat:
Bogdan şi Constantin Hrib,
Marius Dimitriu, Gabriela Mitroi,
Iuliana Nicolau (**Tritonic Media**)

Descrierea CIP a Bibliotecii Naţionale a României
Neliniştile insecurităţii / coord.: Cristian Troncotă. -
Bucureşti : Tritonic, 2005
Bibliogr.
ISBN 973-733-009-9

I. Troncotă, Cristian (coord.)

355.45

Coperta colecţiei: CRISTIAN MATACHE

Tehnoredactare: EXPERT EDIT SRL

Comanda nr. T 202/ februarie 2005
Bun de tipar: 20.11.2004
Tiraj: 1000 exemplare
Tipărit în România

NELINIȘTILE INSECURITĂȚII

Coordonator: Cristian Troncotă

TRITONIC
București

DE ACELAŞI AUTOR:

- *Eugen Cristescu – asul serviciilor secrete româneşti – memorii, mărturii, documente*, Editura Roza Vânturilor, Bucureşti, 1994.
- *Mihail Moruzov şi Serviciul Secret de Informaţii al Armatei*, Editura I.N.I., Bucureşti, 1996.
- *Totalitarismul de dreapta în România. Origini, manifestări, evoluţie 1919-1927*, (în colaborare), Editura Institutului pentru Studiul Totalitarismului, Bucureşti, 1996.
- *Începuturile mişcării de rezistenţă în România, aprilie 1945 - 31 mai 1946* (2 vol. în colaborare), Editura Institutului pentru Studiul Totalitarismului, Bucureşti, 1998-1999.
- *Istoria serviciilor secrete româneşti. De la Cuza la Ceauşescu*, Ed. Ion Cristoiu, Bucureşti, 1999.
- *Ideologie şi formaţiuni de dreapta în România 1927-1931* (în colaborare), Vol. II Editura Institutului Naţional pentru Studiul Totalitarismului, Bucureşti, 2000.
- *Ideologie şi formaţiuni de dreapta în România, vol. III, 5 ianuarie 1931-7 iunie 1934* (în colaborare), Editura Institutului Naţional pentru Studiul Totalitarismului, Bucureşti, 2002.
- *Ideologie şi formaţiuni de dreapta în România, vol. IV, 7 iulie 1934-30 martie 1938* (în colaborare), Editura Institutului Naţional pentru Studiul Totalitarismului, Bucureşti, 2003.
- *Glorie şi tragedii. Momente din istoria Serviciilor de informaţii şi contra-informaţii române pe Frontul de Est (1941-1944)*, Editura Nemira, Bucureşti, 2003.
- *Istoria securităţii regimului comunist din România 1948-1964*, Editura Institutului Naţional pentru Studiul Totalitarismului, Bucureşti, 2003.
- *Duplicitarii. O istorie a Serviciilor de Informaţii şi Securitate ale regimului comunist din România*, Editura Elion, Bucureşti, 2003.
- *Careul de aşi. Serviciile secrete ale Marii Britanii, SUA, Rusiei şi Israelului. O cronică a frontului secret la răspântie de milenii*, (în colaborare), Editura Elion, Bucureşti, 2003.
- *Serviciile secrete ale Franţei, Germaniei, Italiei, Spaniei şi Portugaliei înainte şi după Războiul Rece* (în colaborare), Editura Elion, Bucureşti, 2004.

CUPRINS

Cuvânt înainte 7

I. Mediul internaţional de securitate, factorii de risc, *intelligence*-ul şi problemele de integrare

IULIAN FOTA, Globalizare, integrare şi *intelligence* 13
MONICA ŞERBĂNESCU, Globalizarea, context al îmbinării strategiilor de securitate ale comunităţii internaţionale faţă de provocările ameninţărilor asimetrice 27
AUREL DUMITRU, România în noul context european, coordonate ale securităţii naţionale 78
STELEA COVEI, Ameninţări transfrontaliere la adresa securităţii naţionale 101
DORU COLGIU, Terorismul – risc de securitate globală 116
ALINA TONIGARU, Cyberterorismul – noi provocări 126
ADINA SIMONA APRODU, Factori de risc la adresa securităţii României. Măsuri de contracarare a acestora în primul deceniu al secolului XXI 157

II. Fenomenul corupţiei şi impactul asupra securităţii şi siguranţei naţionale

WILLIAM BRÂNZĂ, Corupţia, o problemă la nivel naţional 179
DIMITRIE BOGDAN LICU, Criminogeneza corupţiei 187
MARIAN LAZĂR, Corupţia – risc major la adresa securităţii naţionale . 197
NELU COMAN, Elemente ale unei strategii anticorupţie eficiente 207

III. Mijloacele de informare şi problemele de securitate şi siguranţă naţională

TUDOR BARBU, Mass-media şi siguranţa naţională 217
FLORIN BRUŞTEN, Mass-media şi securitatea naţională 225

SORANA BELCIU, Rolul presei în apărarea și asigurarea securității culturale 232
CARMEN CREȚU, Mass-media – prelungirea actului terorist 236

IV. Standarde de calitate și protecție

PAUL VIOREL, Armonizarea procedurilor de securitate internă cu standardele și cerințele NATO 251
VALENTINA LUNGU, Managementul informațiilor clasificate – standarde NATO 259
ADRIAN CONSTANTIN, Protecția informațiilor clasificate în România .. 276
ION TRAIAN MIHAI, Securitatea industrială. Experiența nord-americană în domeniul managementului protecției informațiilor clasificate transmise către industrie în cadrul contractelor clasificate 282

V. Alte probleme de securitate și siguranță națională

IONEL LANCIU, Războiul informațional și securitatea națională 291
ROBERT VERESS, Democrația – resursă fundamentală a mediului intern de securitate 312
NARCISA GEORGESCU, Securitatea alimentară componentă a securității naționale 318
MARIAN DUMITRESCU, Drepturile fundamentale ale cetățenilor și activitatea de siguranță națională 326
CLAUDIU LEPĂDATU, Particularități ale activității informativ – operative pentru identificarea vulnerabilităților și factorilor de risc ce pot afecta executarea pazei cu efective de jandarmi 344

VI. Noi abordări, tendințe și reflexii – între tradiție și modernitate

SILVIU NATE, O analiză a tendințelor în managementul de securitate națională 354
CRISTIAN RIZEA, Tinerii și educația pentru siguranță națională 373
VASILE EFTIMIE, Securitatea națională – o abordare comprehensivă .. 385
LIONEDE OCHEA, Comunitatea de informații a României. Tradiție și modernitate 394
DORLIN MUREȘAN, O propunere de evaluare organizațională a României 414

CUVÂNT ÎNAINTE

Prezentul volum reunește studii — dar și analize, eseuri, proiecte — referitoare la o gamă forte variată de probleme ce țin de domeniul siguranței și securității naționale, regionale ori globale. Autorii sunt absolvenții celei de a treia promoții (2004) a Colegiului Superior de Siguranță Națională, curs post universitar organizat de Serviciul Român de Informații prin Academia Națională de Informații.

La propriile experiențe și cunoștințe cu toții au știut să adauge multe din noutățile cu care au venit în contact pe măsura parcurgerii tematicii cursului.

Ca în fiecare an, Colegiul și-a propus cu prioritate să ofere perspective noi în înțelegerea mizelor globale. Din punctul nostru de vedere este o modalitate de a aprofunda, în parteneriat cu societatea civilă, o serie de concepte care devin din ce în ce mai acutizante.

De exemplu, *intelligence*-ul concurențial. Acest concept ar trebui privit în directă conexiune cu necesitatea cooperării și a parteneriatului între instituțiile ce concură la realizarea securității naționale, regionale ori globale, într-o epocă de mari schimbări în raporturile de putere pe arena internațională. Asistăm la un proces de regândire a întregii arhitecturi de securitate națională, în momentul în care România și comunitatea sa informativă sunt înscrise pe traiectorii precise în structurile euro-atlantice. Iar NATO, alianță din care România face parte ca membru cu drepturi depline, începând cu 2 aprilie 2004, reprezintă la ora actuală,

în ciuda unor neajunsuri, instituția internațională care s-a dovedit cea mai flexibilă și capabilă de a evolua pentru a face față cerințelor noului mediu de securitate.

Iată de ce este necesară o educație de securitate, înțelegând prin aceasta cimentarea unei relații de încredere reciprocă între societate și serviciile care-i prezervă starea de siguranță. Chiar dacă există o legătură inextricabilă pe tărâmul asumării priorităților naționale, societatea civilă și structurile informative au, uneori și în statele cu îndelungată tradiție democratică, dificultăți de armonizare, oarecum firesc din cauza naturii particulare a acestor organizații ai căror membri se supun unor norme profesionale ce obligă la o inerentă discreție. Deși este beneficiarul final al stării de siguranță națională, cetățeanul nu cunoaște maniera de funcționare a serviciilor de informații, iar acestora le sunt proprii reguli speciale de acces și utilizare a informațiilor.

Dincolo de reglementările legale, doar înțelegerea adecvată a rolului structurilor cu atribuții în domeniul siguranței naționale în cadrul societății poate constitui premisa unei relații funcționale, mutual benefică.

Deși cursanții Colegiului provin din medii diferite — stat, partide politice, mass-media, organizații neguvernamentale, universități, societăți private, etc.-, sunt cu specializări diferite, de vârste diferite s-a demonstrat și cu această promoție că avem interese comune, că poate exista coeziune. Sunt convins că schimbul de idei și cunoștințele acumulate cu ocazia seminariilor, a meselor rotunde, a călătoriilor de documentare întreprinse, a participării la sesiunea de comunicări științifice a cadrelor didactice din Academia Națională de Informații ori a celorlalte forme de realizare a obiectivelor Colegiului au contribuit decisiv la fundamentarea acestei coeziuni.

Iată de ce ne așteptăm ca și prin această promoție a Colegiului, pe care o putem numi „NATO 2004" să realizăm

împreună acel pas hotărât pentru diminuarea asperităților, care nu poate veni decât din conștientizarea nevoilor celor doi parteneri sociali. Delicata justețe a echilibrului între *transparență* și *secret* nu poate fi decât rodul eforturilor ambilor termeni.

Un serviciu nu poate fi eficient, în limitele deplinei legalități, decât în măsura în care cetățenii pe care-i deservește îl sprijină în demersurile sale. O asemenea atitudine presupune un capital social pozitiv, iar acesta, nu încape îndoială, se dobândește printr-o comunicare eficace. Permanetizarea ei înseamnă instituționalizarea unei formule, unde fiecare află esențialul despre celălalt. Înțelegem că acest Colegiu a devenit deja locul de întâlnire dintre societatea civilă și instituțiile abilitate să-i prezerve siguranța.

Dar, ceea ce transpare foarte ușor din lectura volumului este interesul și seriozitatea de a așterne pe hârtie câteva din propriile gânduri și neliniști, ceea ce dovedește o dată în pus, dacă mai era nevoie, că înțelegerea corectă a problemelor de securitate și siguranță națională reprezintă o chestiune mult prea serioasă pentru a fi ținută în umbra secretului ori a o lăsa pradă ignoranței și superficialității. În fond este vorba despre prezentul și viitorul nostru ori al copiilor noștri.

Suntem pregătiți la nivel național? Mai este important acest lucru dacă privim din perspectiva globalizării? Vom fi oare capabili să înțelegem că dacă vrem liniște, bunăstare și siguranță pentru noi va trebui să acceptăm același lucru și pentru ceilalți? Ce rol va juca *intelligence*-ul de securitate, sau, altfel formulat, va reuși acesta să găsească soluții pentru prevenirea producerii unor catastrofe cu impact asupra umanității? Putem gestiona o situație de criză? Ce rol atribuim mijloacelor de comunicare în masă pre și post eveniment de securitate? Avem un sistem instituțional și legislativ capabile să reacționeze oportun în fața propriilor vulnera-

bilități ori riscuri transfrontaliere? Reprezintă democrația, într-o perioadă de tranziție prelungită, o valoare pentru securitatea națională? Va reuși noul concept de securitate prin cooperare să aducă pacea globală? Este nevoie de un sistem educațional pentru securitate în rândul tineretului? Respectarea standardelor de calitate a produselor, din orice domeniu, are legătură cu securitatea națională? Care sunt standardele internaționale și cât am reușit să le adampăm pe plan național în domeniul protejării datelor, documentelor și informațiilor secrete? Dar în domeniul securității alimentelor? Avem noi românii și ceva pozitiv în tradiția activității de informații care poate fi folositor actualului proces de restructurare instituțională? Cum se respectă drepturile și libertățile fundamentale în activitatea de informații? Iată câteva dintre întrebările formulate, dar și o mai mare varietate de răspunsuri posibile, care toate la un loc dovedesc ținută și rigoare academică alături de o reală responsabilitate civică din partea celor care s-au încumetat să-și dezvăluie neliniștile în paginile acestui volum.

Nu e de mirare că multe dintre studiile acestui volum pornesc de la definirea conceptelor de securitate și siguranță în contextul noilor coordonate ale mediului internațional. Un nou context de securitate în care globalizarea unipolară de acum, ori multipolară, dar limitată strict la nivel regional, după cum se proiectează, a făcut ca, după riposta contra celor bănuiți că poartă responsabilitatea provocării tragediilor din 11 septembrie de la Washington și New York, întregul sistem de drept umanitar internațional, deopotrivă cu instituțiile menite să vegheze la respectarea lui, să-și dovedească lipsa de eficiență. La fel de ineficiente sau dovedit și strategiile planificate până atunci în legătură cu sistemele de apărare, prevenire și contracarare a violențelor (riscurilor, amenințărilor) de tot felul și născute parcă din toate direcțiile, după încheierea războiului rece. Dacă am fi fost și mai riguroși,

nu greșeam prea mult dacă am fi intitulat volumul: *necesitatea regândirii strategiilor și politicilor de securitate în fața escaladării efectelor negative ale globalizării.*

Pentru a schița, măcar în linii generale, noile dimensiuni ale arhitecturii sistemului de securitate globală ce se prefigurează, unii dintre semnatarii studiilor prezentului volum au considerat de interes anticiparea felului în care gândesc, în termenii strategiilor de securitate, factorii cei mai responsabili din marile capitale ale lumii, precum și din zonele adiacente României. Nu a fost omisă nici referirea la stadiul reformelor în domeniul instituțiilor cu responsabilități în culegerea, procesarea și valorificarea informațiilor de securitate, managementul de securitate ori *intelligence*-ul performant. Iar prezentarea analitico-descriptivă între modelul și realizările în plan național față de cele considerate ca fiind de referință pe plan internațional, a urmărit să acopere, măcar în parte, o problematica atât de complexă.

Fenomenul coruției, ca principală vulnerabilitate de securitate națională este și el analizat în paginele volumului, din mai multe perspective: conceptual, legislativ, al stategiilor de prevenire și combatere ori a soluțiilor concrete de menținere a lui la un nivel de suportabilitate.

Fără a te pierde în detalii inutile, parcurgerea problemelor de securitate globală formulează un mesaj foarte clar. Toți factorii de putere implicați și responsabili conștientizează că s-a ajuns într-un moment în care vulnerabilitățile, riscurile neanticipate și nemonitorizate, scăparea de sub control a armamentelor nucleare ori de distrugere în masă, nu se mai pot limita doar la știrbirea poziției, prestigiului și influenței unei singure puteri. Ele afectează viitorul omenirii. Pericolul distrugerii, dacă nu totale, cel puțin a formelor de civilizație modernă, așa cum o cunoaștem astăzi, este real și de neignorat. În fața noilor amenințări nu se mai pot îndrepta „tunurile" (cu înțeles de tehnologii ultraperformante

din domeniul apărării), de către cei care le posedă, dar nici tehnicile atât de perfide ale megaterorismului. Și unii și alții riscă să se afle împreună de partea perdanților, iar în lipsa învingătorilor să aibă parte de ceea ce au semănat. Noile strategii și politici de securitate globală vor fi secondate de un nou sistem de drept internațional umanitar și în consecință de noi instituții naționale și internaționale capabile să facă față noilor provocări.

Departe de noi gânduri fataliste ori vreo intenție disimulată de a nu recunoaște că am fost seduși sau că ne situăm pe baricada celor cu viziuni apocaliptice. Dimpotrivă, încrederea că factorii cei mai responsabili, inclusiv ai societății civile, vor dovedi suficientă inteligență și inspirație în găsirea celor mai potrivite soluții pentru a depăși momentele de criză, nu poate fi abandonată, sub nici o împrejurare. Este exact mesajul prezentului volum. Dar să nu uităm că experiența și mai ales înțelepciunea celor ce știu să învețe din greșelile trecutului, iar istoria stă mărturie și de data aceasta cu suficiente exemple, pot insufla, oricând și oricui de bună credință, doar un optimism suficient de echilibrat, dar nu poate oferi niciodată garanții.

Prof. univ. dr. Cristian Troncotă

I. MEDIUL INTERNAȚIONAL DE SECURITATE, FACTORII DE RISC, *INTELLIGENCE*-UL ȘI PROBLEMELE DE INTEGRARE

GLOBALIZARE, INTEGRARE ȘI INTELLIGENCE

Iulian Fota

Din punct de vedere al garantării securității naționale, România a realizat o performanță ce nu a mai fost atinsă până acum. Pe 2 aprilie 2004 România a devenit membră a Alianței Nord-Atlantice, iar în 2007 pare din ce în ce mai probabil că va deveni și membră a UE. Pentru prima dată în istoria sa România se va afla într-o relație de alianță cu toate statele occidentale importante, inclusiv cu cele ce li se recunosc statutul de mare putere. Va beneficia astfel de garanții de securitate din partea celei mai puternice alianțe militare din lume, NATO, și de sprijinul economic și financiar al celei mai bogate uniuni de state din lume, UE. România, redevenind o țară occidentală, își va relua locul în cadrul lumii occidentale.

Mai mult decât atât, Romania se află într-o relație specială cu SUA, cea mai puternică țară de pe glob și cel mai puternic membru al NATO. Aflat în vizită oficială la București, în noiembrie 2002, președintele Gerge W. Bush afirma: *„should any danger threaten Romania — should any nation threaten Romania, the United States of America and NATO will be by your side*[1]". Relația specială dintre cele două țări,

[1] *President Bush Welcomes Romania to NATO, Remarks by the President to the Citizens of Romania*, Bucharest, November 23, 2002, www.usembassy.ro/Documents/prelBush0211En.htm.

Parteneriatul strategic România — SUA, deja dezvoltat, începând cu 1997, era reconfirmat pe timpul vizitei președintelui Bush la București și confirmat militar și politic în Afganistan și Irak, unde soldații români și-au dat viața alături de cei americani pentru a elimina actuale sau viitoare surse de risc la adresa securității statelor NATO și UE.

Integrarea euro-atlantică a României, pe lângă beneficiul de securitate va avea ca efect și o modernizare rapidă a țării cu influențe faste atât asupra prosperității cetățenilor ei cât și asupra afirmării identității naționale în lume. Astfel, România se va împăca cu globalizarea, adaptându-se noului context internațional din postura de *beneficiar al globalizării* și nu din postura de victimă a ei. La începutul secolului al XXI-lea România nu are a se mai teme cu privire la independență, integritate și suveranitate „țelul istoric al tuturor românilor încă din secolul al XV-lea"[2].

Prin integrarea în NATO și UE România, în numai 14 ani, dintr-o țară izolată atât în Est cât și în Vest[3] va ajunge un important membru al comunității internaționale și un actor cu veleități strategice internaționale. După cum afirma Jamie Shea, „prin integrarea în NATO România se află în același rând cu marile puteri"[4]. Această nouă ipostază va confrunta România cu două mari provocări: 1) valorificarea oportunităților oferite de integrarea în NATO și UE pentru a îndeplinii al doilea mare țel istoric al românilor, transformarea României într-o *țara cu adevarat occidentală, democratică și prosperă*; 2) înțelegerea corectă a noului context internațional global și modernizarea instituțiilor responsabile cu securitatea națională pentru a putea răspunde cerin-

[2] Stephen Fischer-Galați, *Drumul României către democrație: un trecut problematic, un viitor incert, Europa de Est și Războiul Rece*, Institutul European 1996, p 108.

[3] A se vedea interviul acordat în toamna anului 1988, pe timpul vizitei la Washington, de Silviu Brucan lui Nestor Rateș, difuzat la acel moment de Radio Europa Libera și reluat de același post de radio în decembrie 2003.

[4] Interviu ziarul „Jurnalul Național" din luna noiembrie 2003.

țelor de securitate ale integrării euro-atlantice și pentru a asigura României un nou statut internațional.

În superbul său studiu despre drumul României către democrație, istoricul american de origine română, demonstrează clar că „democrația nu este o componentă semnificativă a tradițiilor istorice și politice românești"[5]. Mai mult decât atât, el arată cum în trecut, alianța României cu alte state occidentale (exemplul ales de el este Franța la 1848) nu a dus la „emanciparea țărănimii sau inițierea unor reforme sociale și politice de calibrul și varietatea celor franceze". Mai mult decât atât, spune același Fischer-Galați, „deși platformele politice de la 1848 includeau prevederi în vederea lărgirii drepturilor omului și drepturilor civile, ordinea politică și cea socio-economică urmau să rămână intacte, puterea urmând să fie exercitată aproape exclusiv de membrii mai tineri ai aristocrației"[6].

Poate părea paradoxal, ținând cont de deficitele democrației interne din primii 14 ani de tranziție, dar din ce în ce mai mult România începe să fie altfel receptată atât de statele din zona Europei de sud-est cât și din zona Mării Negre sau a Caucazului de sud. Recent, pe timpul vizitei la București, tânărul și activul președinte georgian, Mihail Saakașhvili, considera România „un posibil model" pentru integrarea ulterioară a țării sale în NATO sau UE.

Aceste două provocări se adresează în egală masură serviciilor de informații din România.

GLOBALIZAREA

Globalizarea descrie o nouă eră care se ridică pe ruinele vechii ere a Războiului Rece. Își trage seva dintr-o economie mondială în curs de a devenii globală sub presiunea dezvoltării accelerate a tehnologiei, în special a celei informatice, a telecomunicațiilor și a transporturilor transcontinentale.

[5] Stephen Fischer-Galați, *op.cit*, p. 107–136.
[6] *Ibidem*.

Globalizarea face din ce în ce mai dificil ca statele să trăiască în izolare unele de altele. Ea erodează rapid granița dintre politica externă și cea internă ca și cea dintre economie și securitate[7]. Globalizarea are multe beneficii, precum accesul mai ieftin la comunicații și transport intercontinental, dar și inconveniente, la acest punct remarcându-se intensificarea acțiunilor crimei organizate transnaționale.

Țările cu guverne democratice pot formula politici mai flexibile și se pot adapta mai ușor la globalizare, devenind astfel beneficiare ale acestui fenomen, pe când țările cu regimuri autoritare sau dictatoriale, fiind mai rigide, devin rapid victime ale ei. Fosta Republică Federativă a Iugoslaviei sau regimul din Irak impus de Saddam Hussein sunt de acum exemple clasice.

Pentru statele lumii și în special pentru statele membre ale NATO și UE provocarea principală este cum să profite de oportunitățile pe care globalizarea le oferă, minimalizând în același timp eventualele riscuri. Un răspuns adecvat la o astfel de provocare necesită o mai bună înțelegere a acestei globalizări și a efectelor sale. De asemenea, reclamă abordări integrate, holistice, în toate domeniile securității naționale.

Globalizarea nu este un proces static ci unul foarte dinamic. Se prezintă în mai multe forme, dintre care numai una este cea economică. Elementele centrale ale globalizării *sunt fluxurile transfrontaliere din ce în ce mai rapide de bunuri, servicii, forță de muncă, bani, tehnologie, informații, idei, culturi, crimă organizată și armament*[8].

Globalizarea nu elimină tradiționalele îngrijorări geopolitice și preocupări pentru securitate. Actorii naționali ca și cei nestatali nu sunt motivați numai de câștiguri economice.

---

[7] Stephen J. Flanagan, *Meeting the challenges of the global century*, din lucrarea *„Challenges of the Global Century :report of the project on globalization and national security"*, Institute for National Strategic Studies, National Defence University, 2001.

[8] Thomas L. Friedman, *The Lexus and the Olive Tree: Understanding Globalisation*, New York,1999.

În egală măsură se păstrează competiția și eventual conflictul pentru teritorii, resurse sau putere. Diferendele militare, etnice sau culturale vin să complice și mai mult acest tablou. Geopolitica globalizării este foarte complexă pentru că în paralel cu globalizarea financiară și integrarea economiilor naționale într-o singură mare economie globală asistăm la fenomene de fragmentare de-a lungul unor linii de fractură regionale și reacții culturale de contra-globalizare. La nivel global șansele unui conflict militar mondial sunt foarte reduse dar pe plan regional anumite regiuni sunt afectate de riscul unor conflicte convenționale sau chiar nucleare semnificative.

Ca urmare a caracterului din ce în ce mai transnațional al principalelor riscuri, în special terorismul și crima organizată, securitatea se bazează din ce în ce mai mult pe cooperare, de unde și evoluția fulminantă a conceptului de *„securitate cooperativă (cooperative security)"*[9].

Din punct de vedere al politicilor de securitate națională, globalizarea obligă statele să-și integreze elementele militare și nemilitare ale puterii. Cheia unui astfel de efort este coordonarea strânsă a domeniilor politic militar, economic, ordine publică, servicii de informații, cultură, știință și tehnică. Oamenii politici ca și strategii militari și civili trebuie să ia mai mult în calcul aspectele de ordin istoric, cultural, tehnologic, religios, ecologic ce intervin în gestionarea noilor probleme de securitate.

Globalizarea produce mai mult decât restructurarea economiei și a comunicațiilor dar redefinește și natura politicii mondiale și a problemelor de securitate. Globalizarea alimentează tensiunile majore care influențează relațiile internaționale: integrare-fragmentare; internationalizare-localizare; centralizare-descentralizare.

În domeniul puterii, globalizarea favorizează apariția de noi centre de putere dintre care *companiile transnaționale*

[9] Richard Cohen, Michael Mihalka, *Cooperative security: new horizons for international order,* The Marshall Center Papers No. 3, 2001.

și *organizațiile ne-guvernamentale internaționale* sunt cele mai cunoscute. Acești noi actori internaționali folosesc din plin avantajele erei informaționale, atât pentru a-și asigura îndeplinirea obiectivelor propuse cât și pentru a-și afirma și consolida prezența în noul joc global de putere[10].

Nu în ultimul rând, alianțele și aliații sunt esențiali în a gestiona aspectele de securitate ale globalizării și a asigura atât succesul eforturilor cât și o notă de plată cât mai scăzută.

INTEGRARE ȘI INTELLIGENCE

Dintre domeniile vieții sociale și politice, domeniul serviciilor de informații este poate unul dintre cele care vor fi cele mai influențate.

În trecut, strategia de securitate a României se formula plecând strict de la considerente de ordin național. Riscurile și amenințările la adresa securității naționale erau definite prin prisma intereselor naționale. Serviciile de informații contribuiau sectorial la întocmirea strategiei de securitate națională și își extrăgeau tot sectorial obligațiile ce le reveneau urmând a-și formula apoi politicile propii.

Ținind cont de specificul domeniului și mai ales de cerințele speciale de protecție a surselor de informare ca și a metodelor de culegere a informațiilor, munca de informații, chiar și atunci când era efectuată în străinătate, avea cel mai pur caracter național.

Integrarea în NATO și UE va veni să modifice procesul conceperii și elaborării strategiei de securitate națională în felul acesta și domeniul serviciilor de informații fiind influențat. Ca membră a NATO și UE securitatea României devine securitatea NATO și a UE, iar securitatea NATO și a UE

[10] Un exemplu classic de acum este folosirea Internetului pentru a convinge opinia publică internațională de necesitatea unui tratat de interzicere a minelor anti-personal.

devine securitatea României. Obligațiile de membru determină acomodarea obiectivelor strategiei de securitate națională a României cu obiectivele Conceptului strategic al NATO și cele ale Strategiei de securitate a UE („strategia Solana").

După 11 septembrie 2001, în viziunea comună a celor două organizații, principalele riscuri și amenințări la adresa securității lumii occidentale o reprezintă terorismul, armele de distrugere în masă, crima organizată și corupția precum și statele slabe, falimentare, „statele bandit"[11]. Pentru a reconfirma acest punct de vedere Colin Powell afirma în fața comitetului pentru relații internaționale al Congresului SUA că „a new reality was born on September 11, a reality that linked terrorists, weapons of mass destruction, and rogue or failed states"[12]. Afganistanul și Irakul sunt doar prime exemple concrete de aplicare comună a acestei convergențe.

Domeniul *intelligence*-ului este astăzi un domeniu prioritar atât pentru NATO cât și pentru UE. NATO are deja o tradiție lungă în a valorifica informațiile culese de statele membre. Pe timpul războiului rece, NATO era dependent în totalitate de informațiile pe care acestea le ofereau. Astăzi NATO continuă să depindă de un astfel de ajutor dar și-a dezvoltat și mijloace propii de culegere de informații, în special pe timpul misiunilor de tip SFOR, KFOR sau ISAF. Din punct de vedere al *intelligence*-ului, NATO nu se rezumă doar la culegere, dar în egală măsură este preocupat și de analiza integrată a informațiilor. Deși unele state aliate au încă rețineri cu privire la confidențialitatea unor astfel de colaborări[13] ele sunt mai mult decât necesare. Recent, mai mulți lideri din Congresul SUA au cerut chiar înființarea

[11] A se vedea „*A secure Europe in a better world*", http://ue.eu.int.

[12] Pledoarie Colin Powell în fața Comisiei de relații internaționale a Congresului SUA, www.state.gov/secretary/rm/2002/13581.htm

[13] Într-o conferință la Centrul de studii NATO din București, mai 2003, William Odom spunea că „*intelligence*-ul multinațional nu este *intelligence*".

unui centru comun de informații SUA — UE *(„joint intelligence center")*, folosindu-se ca model cooperarea interaliată din NATO[14]. Acest centru ar urma să asigure transferul de informații între europeni și americani, subiectul principal fiind terorismul, iar ca zonă de interes *întreaga lume.*

La rândul ei UE, în special în urma adoptării strategiei de securitate, va simți din ce în ce mai mult nevoia unor structuri integrate de analiză și evaluare a noilor riscuri[15], aceste structuri bazându-se pe cooperarea europeană în domeniul serviciilor de informații. Europa are avantajul că deja a făcut pași imporanți în ceea ce se numește cooperarea europeană în domeniul *„criminal intelligence".*

Un ultim argument în favoarea importanței pe care NATO și UE o acordă domeniului serviciilor de informații este recenta conferință de la München. Dintre aspectele cele mai discutate cu privire la îmbunătățirea activității serviciilor aliate de informații s-au remarcat: consolidarea capacităților „Humint"; creșterea calității analizei dar și a personalului specializat în analize; creșterea comunicării între diferitele agenții; îmbunătățirea dialogului între analiști și factorii politici de decizie; orientări politice mai clare[16].

NOUA PARADIGMĂ A INTELLIGENCE-ULUI OCCIDENTAL

Transformările internaționale accelerate de sfârșitul Războiului Rece și conturate astăzi sub forma globalizării anunțau încă de acum câțiva ani o nouă paradigmă de *intelligence.* Tragicele evenimente teroriste de la 11 septem-

[14] Douglas Farah, Dan Eggen, *Joint intelligence center is urged,* în „The Washington Post", 21 decembrie 2003.

[15] Fraser Cameron, *An EU strategic concept,* în „Transition Studies Review", 1/2003.

[16] *NATO on the road to Irak,* The 40th Munich conference on security policy, www.worldsecuritynetwork.com.

brie 2001, de la New York și Washington, nu au făcut decât să confirme tezele analiștilor din serviciile de informații care prevesteau ceea ce se întâmplă astăzi.

Paradigma clasică a *intelligence*-ului avea ca esență a sa teza potrivit căreia principalii competitori sau dușmani ai statelor sunt alte state. Sarcina principală a oricărui serviciu de informații era să monitorizeze atent celelalte state și elementele de putere ale acestora. Scenariul cel mai periculos cu putință era cel al agresiunii militare al unui stat împotriva altui stat. NATO a fost creat pentru ca în acest fel statele membre să descurajeze o eventuală agresiune a URSS la adresa statelor occidentale sau, în caz că aceasta avea loc, să-i poată face față.

Nici unul din membrii fondatori ai NATO nu și-ar fi imaginat vreodată că alianța va invoca pentru prima dată în istoria sa articolul 5, în urma unui atac terorist. Atacul asupra lui World Trade Center și Pentagonului a fost ultimul argument în a determina comunitatea euro-atlantică de informații să propună o nouă paradigmă a activității de informații[17]. În esență, această nouă paradigmă propune: prioritara să fie monitorizarea „statelor bandit" (*rogue states*) și a entităților criminale nestatale; cauzele comune să primeze chiar și în balanță cu obținerea unor avantaje naționale competitive; sprijin direct pentru acțiunile multilaterale; dezvoltarea de mecanisme de cooperare internațională în domeniul serviciilor de informații, dar numai în domeniul analizei și al evaluării, nu și în cel al culegerii de informații (culegerea informațiilor se păstrează în continuare ca o prerogativă eminamente națională); obiectivitatea și controlul democratic devin trăsături caracteristice ale unei „bune guvernări". O subliniere aparte merită cuvântul „obiectivitate", care în spirit anglo-saxon înseamnă a-i spune guvernului și ce nu-i place să audă.

——— [17] Michael Herman, *11 September: legitimising intelligence?*, Conflict Studies Research Centre, august 2002.

IMPLICAȚII PENTRU SERVICIILE ROMÂNEȘTI

Nevoia de a contribui în mod eficient la îndeplinirea obiectivelor NATO și UE ca și nevoia de a armoniza aceste obiective cu cele naționale va ridica în fața serviciilor de informații din România două categorii de provocări.

Prima este legată de nevoia de a înțelege corect contextul internațional în care toate aceste procese au loc și tendințele principale de evoluție din sistemul internațional. Din ce în ce mai mult, analiștii de relații internaționale definesc actuala etapă de dezvoltare a relațiilor internaționale drept „globalizare"[18].

A doua mare provocare se referă la cerințele adaptării profesionale a serviciilor de informații din România la efortul colectiv transatlantic de combatere a noilor riscuri și amenințări. Această adaptare va necesita în egală măsură evaluarea de noi concepte care să stea la baza muncii de informații cât și revizuirea arhitecturii sistemului național de informații și în special crearea „comunității naționale de informații".

Serviciile de informații românești au depus eforturi în ultimii ani pentru a răspunde atât noilor cerințe profesionale cât și celor ținând de democratizarea vieții politice din România. În perioada următoare, serviciile românești vor trebui să facă față unei triple game de cerințe, de decurg din: nevoile de reformă, în primul rând combaterea corupției; evoluțiile geopolitice din zonele adiacente României; obligațiile noastre de membrii NATO și viitori membri ai UE.

Pentru a putea face față cu succes acestor cerințe, serviciile de informații vor trebui să concentreze mai multe eforturi și resurse pe câteva direcții prioritare.

O primă direcție ar putea fi legată de asigurarea unei minime interoperabilități intelectuale cu celelalte servicii de informații din Occident, prin preluarea termenului de

[18] Challenges of the Global Century:report of the project on globalization and national security, Institute for National Strategic Studies, National Defence University, 2001.

„intelligence" și folosirea lui ca atare. Avantajul este ca, prin semnificația sa, el reușește să acopere mai bine domeniul la care ne referim ca și natura activităților cuprinse aici. Conform literaturii de specialitate, prin *„intelligence"* se înțelege cunoașterea, organizările și activitățile care rezultă prin[19]: culegerea, analiza, producția, diseminarea și exploatarea specializată a informațiilor referitoare la orice alt guvern, grup politic, partid, mișcare sau organizații militare sau paramilitare care se crede că ar putea avea vreo influență asupra securității țării respective; neutralizarea sau contracararea unor activități similare din partea unor alte guverne, grupuri sau mișcări; acțiunile acoperite întreprinse pentru a schimba comportamentul sau chiar componența unor astfel de guverne sau grupări.

Sintetic, activitățile de mai sus pot fi grupate în patru categorii: culegerea informațiilor, contrainformațiile, analiza și acțiunile acoperite. Echivalentele din limba română, respectiv termenii de „informații" sau „servicii de informații" nici pe departe nu sunt atât de cuprinzători.

O a doua direcție ar fi creșterea capacității de analiză și de evaluare. În ziua de astăzi, orice societate occidentală se scaldă într-un ocean de informații. Ne aflăm în epoca surselor deschise, iar Internetul ne oferă acces la biblioteca virtuală a omenirii. Doar calitatea intelectuală a analiștilor și eficiența sistemelor de gestiune a informațiilor face ca, în final, să poți pune pe masa factorului de decizie informația necesară, la momentul oportun și în formatul care să o facă inteligibilă. În Occident avem a doua mare transformare a domeniului serviciilor de informații[20].

O a treia direcție trebuie să fie îmbunătățirea cooperării între serviciile naționale de informații. În statele totalitare

——— [19] Roy Godson, *Intelligence and security*, în "Security Studies for the 21st Century„ Brassey's 1997, p. 325.

[20] Douglas H. Dearth, *National intelligence: profession and process*, în „Strategic Intelligence: theory and application", US Center for Strategic Leadership, 1995.

instituțiile aparținând de sistemul securității naționale erau organizate și acționau în baza vechiului principiu roman „divide et impera"[21]. În acest fel dictatorul le putea ușor juca pe unele împotriva celorlalte, controlând astfel sistemul. În astfel de condiții, cooperarea între acestea lăsa de dorit, și, mai mult decât atât, pe termen lung se ajungea la formarea unor „adevărate state în stat". România nu a făcut excepție de la acest model și poate că cea mai bună dovadă este evoluția sistemului de securitate națională după evenimentele din 1989, când noile autorități constituționale acționează în baza aceluiași principiu, ajungând astăzi să avem de exemplu nouă servicii de informații dintre care patru de nivel național și cinci departamentale. Deși cooperarea între aceste servicii s-a îmbunătățit, un rol extrem de important jucându-l cerințele legate de integrarea în NATO și UE, ea este departe de a fi satisfăcătoare. Suprapunerea de responsabilități, în special în domeniul terorismul sau al combaterii corupției și al criminalității economico-financiare (poate cele mai bune exemple), generează nu de puține ori dispute mai mult sau mai puțin publice între serviciile de informații din România. Uneori aceste dispute capătă accente paroxistice, fie punând în pericol acțiunile profesionale derulate de aceste instituții (precum cazul Terasa Anda) fie inducând semnificative semne de îngrijorare cu privire la rolul politic al acestor servicii. Un exemplu recent, extrem de negativ, este și disputa derulată în jurul arestării generalului doctor Blaj și reproșurile adresate între serviciile de informații ale MApN și MI, reproșuri ce l-au determinat pe ziaristul Radu Tudor, fin observator al problemelor de *intelligence* și al celor legate de instituția serviciilor de informații, să anunțe un posibil război al serviciilor secrete[22].

[21] Dr. Theodor Winkler, *Adaptation of security structures to contemporary threats*, DCAF-working paper no.137, 2004, p 3.

[22] Radu Tudor, *Reîncepe războiul serviciilor secrete*, în „Ziua", 18 mai 2004, p. 4.

O a patra direcție este definită de reglementarea relațiilor cu societatea civilă, care continuă să fie suspicioasă și neîncrezătoare, atât în echidistanța serviciilor de informații cât și în profesionalismul lor. O dovadă la îndemână este reacția unor personalități politice sau civice la introducerea de către firma CONEX a programului „BUSOLA". O simplă decizie tehnică, inerentă unui astfel de sistem, a fost percepută ca o tentativă de monitorizare a mișcării posesorilor de telefoane de către serviciile de informații. Societatea civilă se teme că serviciile se amestecă în politică și influențează principalele decizii politce și economice mai mult decât este firesc. Cazuri precum FNI, îi susțin această teamă. Pe de alta parte, serviciile de informații au nevoie de o relație foarte bună cu societatea civilă din două motive: se legitimează eforturile lor, societatea civilă reprezentând contribuabilul; se creează condiții mai bune pentru edificarea unei relații de încredere între serviciile române și omologii lor din Occident, fiind relativ dificil să ceri să fii credibil în Occident cât timp în propria ta țară și în fața propriei tale opinii publice nu te bucuri de încredere sau apreciere.

O a cincia direcție prioritară ar trebui să fie dezvoltarea unei noi culturi a relațiilor internaționale și în special a culturii globalizării. Înțelegerea corectă a acestui fenomen nu numai că ar spori calitatea analizelor, dar ar spori și zestrea informativă a diferitelor servicii. Nu trebuie uitat că încă din 1977 s-a inventat termenul de *„intermestic"*, tocmai pentru a dovedii că între extern și intern interdependența este tot mai strânsă. Analiza și înțelegerea fenomenului de globalizare trebuie ferită de orice fel de deformări ideologice pentru a nu ajunge la concluzii eronate. Trăim o epocă de radicale schimbări conceptuale și foarte pragmatică abordare a problemelor de securitate internațională. Principiul neamestecului în treburile interne nu l-a putut salva pe Saddam Hussein așa după cum nu i-a putut salva nici pe Slobodan Miloșevici sau chiar pe Nicolae Ceaușescu.

Ultima direcție, dar nu cea din urmă, este cea a personalului și nu atât nivelul salarizării este cel important, cât cel al unei noi morale și etici profesionale. În domeniul ser-

viciilor de informații, patriotismul trebuie să fie profesionalism în slujba țării și nu în slujba unui partid sau a anumitor grupuri de interese. Cuvinte precum *„onoare, datorie, curaj, sacrificiu"* se impun a fi prețuite la adevărata lor valoare. Noul context internațional este unul foarte dur, iar condițiile în care specialiștii serviciilor române de informații își vor desfășura activitatea nu sunt deloc blânde. Poate că cel mai puternic argument în favoarea acestui punct de vedere este să reamintim sacrificiul celor doi subofițeri români în Afganistan, care, facând parte din trupele de cercetare, ar putea fi considerați în egală măsură sacrificii în slujba patriei ale noului *intelligence* românesc.

CONCLUZII

Tema dominantă a secolului XX a fost lupta democrațiilor occidentale împotriva totalitarismului. Efortul a fost atât de intens și miza atât de mare încât, sub impactul entuziasmului victoriei, un universitar american lucid precum Fukuyama s-a grăbit să afirme „sfârșitul istoriei". Din păcate, atentatele teroriste de la 11 septembrie 2001 de la New York și Washington ori de la 11 martie 2004 de la Madrid au venit să infirme așteptările optimiste și, dimpotrivă, să afirme faptul că istoria este mai vie ca oricând. România, alături de statele occidentale, trebuie să răspundă eficient noilor riscuri și amenințări. Pentru secolul XXI aceeași comunitate democratică, occidentală, va trebui să găsească o cale de a gestiona haosul strategic care se extinde la granițele sale de sud și de est. Dacă în secolul trecut importanța era *„securitatea în Europa"*, în secolul care abia a început devine crucială *„securitatea pentru Europa"*. În acest efort colectiv serviciile de informații au rolul și locul lor bine determinat. Ceea ce este foarte important de reținut este faptul că serviciile române de informații au șansa unei a doua tinerețe și pentru prima dată după 1947 au șansa unei recunoașteri internaționale corecte.

GLOBALIZAREA, CONTEXT AL ÎMBINĂRII STRATEGIILOR DE SECURITATE ALE COMUNITĂȚII INTERNAȚIONALE FAȚĂ DE PROVOCĂRILE AMENINȚĂRILOR ASIMETRICE

Monica Șerbănescu

„Lorsque vous traitez un sujet il n'est pas
toujurs nécessaire de l'épuiser,
il suffit souvent d'y faire penser".

(Montesquieu)

Creșterea interdependenței în relațiile internațională generată de globalizare, care este deja „un proces ireversibil, deopotrivă benefic prin incidența lui cu economicul, dar susceptibil să creeze disfuncționalități sociale" cum susținea Anthony Giddens, a adus și noi aspecte ale noțiunii de *„securitate națională și internațională"*[23]. Giddens afirma că *„Globalizarea poate fi definită ca intensificarea relațiilor sociale extinse la scara lumii întregi prin care se leagă locuri dispuse la mare distanță astfel încât ceea ce se petrece la nivel local este afectat de evenimentele care au loc la mii de mile distanță și viceversa"*[24].

În opinia altui autor globalizarea este *„răspunsul american la încercările europenilor și japonezilor de a se găsi ca parteneri de dialog la aceeași masă cu SUA"*[25].

---

[23] Anthony Giddens, Runoway World, Londra 1999 citat de prim ministru, Adrian Năstase, cu prilejul Conferinței cu tema *"Domesticirea globalizării și buna guvernare"* susținută la 18 decembrie 2003 în Aula Academiei Române„

[24] Anthony Giddens, Jan Aart Scholte, *The globalization of World Politics*, p. 15

[25] K. Melos, *Globalizarea. O nouă formă de internaționalizare a economiei. Mituri și realitate*, Atena, 1999, p. 68.

Pentru Ghibuțiu, globalizarea reprezintă procesul deosebit de dinamic al creșterii interdependențelor dintre statele naționale, ca urmare a extinderii și adâncirii legăturilor transnaționale în tot mai largi și mai variate sfere ale vieții economice, politice, sociale și culturale, având drept implicație faptul că problemele devin mai curând globale decât naționale, cerând la rândul lor o soluționare mai curând globală decât națională[26].

Procesul de globalizare caracterizat prin interdependența, interacțiunea, simultaneitatea, incertitudinea, instabilitatea și dinamica ridicată a evenimentelor a avut ca rezultat societatea informațională văzută ca o realitate fără granițe naționale în care facilitățile digitale, de la comunicații prin fibre optice până la sateliți și software de ultimă oră se îmbină cu o gamă diversificată de influențe negative, riscuri și amenințări la adresa securității indivizilor, țărilor sau planetei.

GLOBALIZAREA ȘI NOILE RISCURI DE SECURITATE

Sfidările induse de procesul globalizării, suprapunerea acestuia cu tendințele spre regionalizare și fragmentare au generat noi tensiuni și factori de risc. Multiplicarea continuă a numărului de entități ce acționează pe scena politică globală prin afirmarea factorilor nestatali a condus la creșterea dificultăților de luare a deciziilor în politica externă și de securitate a statelor. Acestor sfidări trebuie să li se răspundă prin noi forme de solidaritate capabile să gestioneze un spectru larg de tensiuni, riscuri și o gamă variată de manifestare a acestora, cum sunt: tensiunile etnice, terorismul, instabilitatea politică a unor zone, reîmpărțirea unor zone de influență etc.

[26] Adrian Victor Ververa, *Societatea civilă și securitatea națională*, în *Meridiane de securitate*, Editura A.N.I., București 2004, p. 43–45.

Opiniile exprimate de politologi și analiști în ultimul deceniu al secolului al XX-lea au identificat efecte alarmante ale globalizării care au adus în centrul atenției comunității internaționale probleme precum: comunicațiile, armele convenționale, corupția, asistența pentru dezvoltare, finanțele globale, comerțul internațional, conflictele intrastatale, sănătatea, drepturile omului, comunicarea globală, conservarea naturii, armele nucleare, biologice și chimice, poluarea, refugiații, crima organizată transfrontieră și terorismul.

Aceste vulnerabilități impuse de globalizare au creat nu numai noi medii conflictuale, noi riscuri și amenințări dar și dimensiuni inedite de răspuns din partea politicilor de securitate care presupun dezvoltarea unor capabilități de gestionare a crizelor și de derulare a operațiunilor multifuncționale adaptate atât părții vizibile a *„icebergului infracțional"* cât și zonei subacvatice a acestuia.

Din această perspectivă guvernele asigură interoperabilitatea conceptual-organizatorică și instituțională pentru protejarea teritoriului național și a valorilor supreme în statul de drept, cu accent asupra drepturilor și libertăților fundamentale ale cetățenilor. Eforturile autorităților vizează identificarea și evaluarea naturii, ariei de extindere a surselor de risc și a consecințelor ce pot surveni, precum și aplicarea unor mecanisme și proceduri, atât de reducere a riscurilor, cât și de intervenție unitară, planificată pentru descoperirea, neutralizarea și anihilarea faptelor sociale atunci când amenințările au evoluat la acest stadiu.

Analizele de vulnerabilitate bazate pe mecanisme și proceduri de management de risc evidențiază faptul că, dacă din perspectiva apărării colective, nivelul de vulnerabilitate a statelor este în scădere, participarea la impunerea politicilor regionale sau multinaționale de securitate mărește gradul de expunere a statelor la amenințări asimetrice[27].

——— [27] Gheorghe Boaru, Marcel Răducu și Vasile Păun, *Managementul riscurilor în acțiunile militare*, Editura Academiei de Înalte Studii Militare, București, 2003, p. 12–23.

O abordare a fenomenelor, bazată pe mecanisme și proceduri de management de risc concretizate în identificarea, analiza, planificarea, monitorizarea, controlul și comunicarea riscurilor, asigură evitarea surprinderii, creșterea probabilității ca evenimentele să se producă în conformitate cu așteptările, translatarea accentului de pe gestionarea crizei pe prevenirea ei în scopul facilitării luării deciziilor de către factorii abilitați, ce se confruntă cu provocările globalizării, această imprevizibilă paradigmă a civilizației secolului al XXI-lea.

Marile discrepanțe constatate în nivelul de dezvoltare economică care se accentuează tot mai mult în condițiile unor progrese tehnologice fără precedent, accesul discriminatoriu la educație și protejarea sănătății, la resursele esențiale ale vieții, la informație și cunoaștere, provoacă grave crize sociale, generează frustrări și stârnesc nemulțumiri. În condițiile globalizării crizele sociale sunt însoțite de cele mai multe ori de crize de identitate, generatoare de violențe neașteptate.

În opinia unor analiști sociali se apreciază că cea mai importantă criză se referă la modul de viață al omului, la identitatea sa și la concepția sa privind societatea[28].

Oportunitățile oferite de globalizare și deschiderea societății civile au oferit o multiplicare nu numai a intereselor naționale dar și a celor promovate de anumite grupuri religioase sau etnice, ce au acționat deschis sau ocult pentru apărarea drepturilor lor împotriva unor discriminări economice și politice.

Se poate vorbi de o adevărată explozie a crizelor de identitate conturate de acțiunile grupurilor tradiționale — mai nou sprijinite ferm de diasporele etnice sau religioase din străinătate — care au pus la grea încercare eforturile de guvernare. Unele state au fost puse în dificultate, datorită

——— [28] M.Albrow, Auf dem Weg zu einer globalen Gesellschaft, Perspectiven der Weltgesllschaft, Ed. U.Beck, Frankfurt am Main, 1998, p. 422 și U.Beck „Ce este mondializarea„, Atena, 1999, p. 224.

capacității lor, din ce în ce mai scăzute, de a îndeplini funcțiuni esențiale în mod autonom, în condițiile în care acest gen de amenințare le-a afectat, atât modul de concepere a securității, cât și modul practic de realizare a politicii de securitate.

Se poate vorbi în prezent de existența unei corelații între naționalism (conturat prin ignorarea în politicile naționale a identităților etnice diferite) și resurecțiile religioase sau chiar decreștinarea apărută în unele regiuni (ex. populația româno-vlahă din nord-estul Serbiei, ca o consecință involuntară a intervenției bisericii creștin-ortodoxe, care refuză dreptul comunității ortodoxe de a se manifesta religios, pentru că nu împărtășește aceeași identitate etnică)[29].

Acțiunile grupurilor etnice sau religioase au reprezentat nu numai o sfidare la adresa autorităților dar și un pericol geopolitic major și mereu în actualitate dat de creșterea eterogenității în aproape toate statele care se confruntă cu noile dimensiuni ale migrării și răspândirii unor religii, precum cea creștină și islamică. Îngrijorător este și faptul că antioccidentalismul musulman este în creștere și se manifestă concomitent cu amploarea sensibilizării lumii occidentale față de pericolul islamic. Aceste grupuri religioase în continuă extindere, prin atragerea constantă de noi adepți, sunt implicate în susținerea unor cauze politice sau finanțarea unor grupări non profit, ale căror interese subterane pun în pericol stabilitatea economică, socială și politică a unor state.

Îngrijorător, pentru state, este faptul că mișcările religioase și acțiunile unor grupuri etnice[30], ce-și păstrează

[29] Dan Dungaciu, *Geopolitica ortodoxiei si resurecțiile etno-religioase în sud-estul Europei, cazul Serbiei, Muntenegrului, Ucrainei și republicii Moldova*, a-X- a Sesiune de comunicări științifice, *Securitate și societate, provocările mileniului trei. Secțiunea Istorie și geopolitică*, Editura A.N.I., București, 2004, p. 105.

[30] Se estimează că la începutul secolului al XXI-lea numărul de grupări etnice distincte din punct de vedere lingvistic este de aproximativ 5000, ce concentrează atât grupurile mici care trăiesc în zone izolate dar și cele mari situate pe meleagurile ancestrale și în diasporă. A se vedea Ion Stan, *Considerații privind problematica intereselor naționale în*

identitatea culturală în devenirea istorică, își concentrează atenția pe promovarea manipulării genetice, pe invocarea unor decalaje între veniturile dintre bogați și săraci, efecte ale unei ineficiente politici guvernamentale sau bazate pe noul curent euroasiatic.

Se pare că proiectul noului euroasiatism al Rusiei, axat pe ruptura civilizației europene de legăturile cu Statele Unite pentru o eventuală alianță a vest-europenilor cu Rusia dar și cu lumea islamică și zone precum India și China, întâmpină rezistența creștin-democraților și conservatorilor europeni, care vor ca frontierele definitive ale Uniunii Europene să fie până la Federația Rusă.

Moscova agreează extinderea Uniunii Europene, situație în care ar dobândi o poziție specială prin conturarea unei relații strategice cu o Europă Unită în condițiile formării unui sistem de apărare în afara parteneriatului transatlantic, a cărui extindere nu este privită favorabil.

Unii autori au considerat că, o posibilă explicație a crizelor de identitate, ar fi influența și efectele supranaționalului asupra microregionalului în sensul că supranaționalitatea determină revendicări naționale ori regionale, ceea ce înseamnă că mondializarea va accentua procesul divizării. Un astfel de exemplu inedit, apărut în era globalizării, a fost noul tip de violență specific Africii de sud și Europei de est, în perioada anilor 1980–1990. Acest nou tip de conflict violent, descris ca un război intern post-modern, de intensitate redusă, dar cu largi implicații internaționale, s-a delimitat de războiul tradițional, crima organizată și acțiunile obișnuite de nerespectare a drepturilor omului.

Fenomenul menționat a adus în prim plan „politica identităților" generată de sărăcie, ineficiența politicilor de guvernare, corupție, amploarea manifestărilor violente ale

——— *condițiile globalizării*, A X-a Sesiune de comunicări științifice, *Securitate și societate: provocările mileniului trei*, Secțiunea: Securitate și siguranță națională. Securitatea la începutul mileniului III, Editura A.N.I., 2004, p. 80–81.

criminalității organizate, apariția grupărilor paramilitare și dispariția legitimității politice, aspecte care au constituit o nouă sursă de tensiune și îngrijorare pentru politicile de securitate adoptate de state.

Interdependența crescândă a societăților, intensificarea legăturilor transnaționale și pluriapartenențele pe care acestea le generează au dus și la apariția unor tensiuni între naționalitate și cetățenie. Pe de-o parte, cea care există între caracterul de universalitate al principiilor democratice ale cetățeniei și relativele restricții — în cea mai mare parte a țărilor — în aplicarea multora dintre aceste principii numai față de naționali, și, pe de altă parte, contradicția dintre declarațiile în favoarea drepturilor omului, pe care statele democratice le folosesc adesea în politica externă și apărarea interesului național care inspiră această politică.

În acest context, dinamicile transnaționale impun cerințe noi de aplicare a idealului cetățeniei și conturarea unor modalități democratice de organizare socială și politică, de cooperare între state care să permită o protecție a exercitării drepturilor și libertăților fundamentale ale indivizilor[31].

Globalizarea nu a diminuat rolul statului național în gestionarea economico-socială ci i-a accentuat importanța și flexibilitatea în adoptarea unor soluții de rezolvare a crizelor de identitate în spațiul național, unde au fost facilitate relațiile de apropiere dintre oameni, diminuate sau anulate separările etnice sau de altă natură cu luarea în considerație a liantului oferit atât de folosirea unei limbi comune dar și a apartenenței la aceeași religie.

Statele naționale își pierd uneori din putere și suveranitate prin eforturile de creare la nivel regional a unor unități multietnice superioare pentru controlul căreia se promovează o putere mondializată bazată pe agențiile de aplicare a legii.

——— [31] Michel Girauld, *Etnicitatea ca necesitate și ca obstacol*, în *Cetățenie și integrare socială* (e.d.) Gilles Fereol, Editura I.N.I. București, 1999, p. 58.

Instrumente foarte puternice pentru impunerea și păstrarea acestei puteri în lume sunt informatica și mediile de informare. Prin intermediul acestora, informațiile sunt adunate din lumea întreagă și oferite lumii întregi. Întreaga omenire devine o vecinătate, o piață care poate să fie controlată și condusă într-un mod nevăzut[32].

Informația și comunicarea au ieșit din ceea ce Daniel Bougnoux a numit *„grafosferă"*, care își exercită funcțiile și produce efectele prin noile mijloace: radioul, televiziunea și mai nou rețelele și „autostrăzile" informației, astfel încât același autor francez afirmă că se îndreaptă spre o „ciberdemocrație" care extinde spațiul public la cel planetar, iar „această comunicare virtual universală, fără nici o dirijare a sensului, anunță sfârșitul lumii", adică al unei lumi „în care se încurajează diversitatea culturilor, a sensibilităților și a cunoștințelor, în care *web*-urile reprezintă o depășire a formei enciclopedice tradiționale și propun un enciclopedism de o altă factură"[33].

Prin fuziunea informaticii cu telecomunicațiile, birotica, robotica etc. a luat naștere un conglomerat de industrii și servicii cunoscute și utilizate ca tehnologie informațională sau tehnologia informației și telecomunicațiilor, în prezent Internetul fiind una dintre cele mai valoroase surse de informații din întreaga lume.

În societatea informațională, informația reprezintă elementul cheie ce trebuie manipulat în avantajul acelora care încearcă să influențeze cursul evenimentelor[34]. Informația constituie o dimensiune funcțională distinctă a conflictelor dintre actori care transformă războiul informațional într-un „război silențios" a cărui strategie utilizează mijloace tehnice

[32] Georgies I. Mantzaridis, *Globalizare și universalitate. Himeră și adevăr*, Editura bizantină, București, 2002, p. 17.

[33] Monica Șerbănescu, Ilie Botoș, Dumitru Zamfir, *Low & Crime. Net*, Editura Tritonic, București, 2003, p. 34.

[34] Vasile Păun și Cristina Pop, *Inteligence competitiv. Un alt mod de a gândi în afaceri*, Editura U.T.I., București, 2003, p. 14.

sofisticate pentru controlul, anihilarea și neutralizarea adversarului, printr-o superioritate informațională, de regulă, evitându-se recurgerea la o confruntare armată directă. În acest context, războiul a suferit o deplasare spre noi câmpuri de interes din domeniile economic, politic, militar, informațional al rețelelor de infrastructură, în cadrul cărora globalizarea reprezintă termenul de referință[35].

Informația a devenit un factor dominant în toate domeniile de activitate fiind nu numai o armă de temut în mâinile celor care o dețin și știu să o folosească dar și o țintă a operațiunilor de colectare, derulate de persoanele sau instituțiile interesate. Deținerea informației este sursa hegemoniei. SUA controlează mai mult de 80 % din fluxul de informații. Pentru eficientizarea utilizării informației ca armă se apelează la alterarea directă a informațiilor sau interzicerea accesului competitorilor la acestea, pe de altă parte poate fi compromisă tehnologia colectării, stocării și diseminării informațiilor. Utilizând alte tehnici mai subtile poate fi schimbat modul de interpretare a datelor, prin alterarea contextului în care acestea sunt prezentate.

Mediul de securitate aflat într-un raport de intercondiționare cu informația, ca element structural al acestuia este supus unor amenințări multiple între care agresiunea informațională reprezintă tipul de pericol care folosește ca armă informația, pentru a ataca ținte sensibile, precum procesorii sociali de informații — oameni, organizații sau comunități umane — în scopul producerii unor perturbări sau distrugeri a funcționării activității pe care aceștia le desfășoară, a inducerii unor stări de dependență față de puterile agresoare ori a pierderii specificității acestora, acțiuni la care își aduc uneori concursul deliberat și mijloacele de informare în masă.

A apărut astfel noțiunea de „protecție a informațiilor", concept complex care cuprinde ansamblul de măsuri necesare pentru a preveni oricare din atacurile posibile, cripto-

——— [35] Vasile Păun, Anca Monica Popa, *O provocare strategică: războiul informațional*, Editura U.T.I., București 2002, p. 31.

grafia fiind una din soluțiile pentru contracararea acestora. Realizarea unui sistem de protecție a informațiilor cuprinde două componente importante: sistemul de protecție, compus din aparatură la care se adaugă luarea unor măsuri eficiente organizatorice și de control; evaluarea siguranței oferite de sistemul constituit, față de riscurile probabile.

Tehnologia sofisticată deschide posibilități multiple de săvârșire a noi categorii de infracțiuni și distruge uneori intimitatea, lezând echilibrul dintre nevoia de protejare a vieții și securitate publică. Calculatorul dă posibilitatea anonimilor de a afla mai multe informații despre o persoană fără consimțământul acesteia, victima fiind pusă în situația de a nu ști ce se cunoaște despre ea într-o lume digitală în care există doar o aparență de intimitate, confidențialitate și drept la libera exprimare a utilizatorilor.

Pentru hackerii cu abilități în domeniul computerelor există o piață vastă cu secrete comerciale și de securitate care pot fi accesate și transmise electronic. În plus, comunicațiile multiple care reprezintă o caracteristică de bază a Internetului, permit producerea și transmiterea pe scară largă de informații și date, care pot fi dăunătoare prin incitarea la violență sau pot constitui chiar amenințări la adresa siguranței naționale.

Tehnologiile specifice informației: de înregistrare audio, video-digitale, cyberspațiu, e-mail, g.s.m., a telecomunicațiilor și a altor manifestări externe ale cetățeanului devin din ce în ce mai periculoase pentru libertatea de expresie, prin anihilarea voinței sale libere, sugrumând treptat însuși spiritul liber care constituie temeiul societății.

Cu toate acestea statul, prin organele judiciare abilitate, acționează în condițiile prevăzute de lege, iar atunci când sunt date sau indicii temeinice privind pregătirea sau săvârșirea unei infracțiuni, pentru care urmărirea penală se efectuează din oficiu, se impune, pentru aflarea adevărului în scopul tragerii la răspundere penală a făptuitorilor, în cazuri bine justificate, luarea măsurii de restrângere tem-

porară a exercitării unor drepturi și libertăți fundamentale ale cetățenilor.

Amestecul unei autorități publice în exercitarea, de exemplu, a dreptului la respectarea vieții private și de familie, este permis, potrivit art.8, pct.2 din C.E.D.O., numai „în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății și a moralei ori protejarea drepturilor și libertății altora".

În acest context, statele trebuie să facă eforturi pentru contracararea criminalității informatice în continuă creștere prin supraveghere electronică, elaborarea unor norme juridice eficiente în cyberspațiu la nivel internațional, prin adoptarea unor politici și metode de contracarare a fenomenului, care să țină seama de scopul moral al acțiunilor întreprinse de necesitatea protejării ordinii publice, a bunelor moravuri, a vieții private și a altor drepturi fundamentale ale cetățenilor care pot fi atacați în spațiul virtual, unde „țipătul" victimelor nu are șansa de a fi auzit niciodată.

Societatea umană devine tot mai complexă ca structură, ca rol, ca proiecție grupală fiind indisolubil legată de fenomene ce au ca nucleu idei precum: securitate, globalizare, aderare, geopolitică, integrare, protecție, „state tampon", federalizare, etnicitate, terorism, minorități semnificative, educație publică, identitate europeană etc. Toate ar putea constitui virtuale provocări de studiu ținând cont și de faptul că evoluția societății în viitor ar putea valida realismul și eventual legitimitatea lor și a implicațiilor acestora la nivel mondial[36].

——— [36] Ruxandra Răscanu, Ruxandra Aldea, Barbara Crăciun și Alina Manolache, *„Profilul Suprapus" al cerințelor și expectațiilor diplomatice din perspectiva de aderare a României la NATO și UE*, a X-a sesiune de comunicări științifice, *Securitate și societate, provocările mileniului trei*", Secțiunea Psihologie și psihopedagogie și metodică, Editura ANI 2004, p. 19.

De asemenea, accesul relativ ușor la noile tehnologii în domeniul comunicațiilor și al transporturilor au determinat realizarea unor contacte directe și a unor formule consistente de cooperare între diferite țări, regiuni și civilizații de pe glob. În egală măsură aceleași mijloace pot deveni vectori de proliferare și transmitere foarte rapidă a noilor riscuri și amenințări.

O întreagă literatură a fost dedicată în acest context riscurilor asimetrice, ce pot pune în pericol securitatea cetățenilor și capacitățile instituțiilor statelor abilitate să adopte politici de asigurare a securității prin abordări integratoare a mediului intern și extern în contextul unor acțiuni de cooperare conjugate la nivel internațional. Expresiile război asimetric, amenințare asimetrică, conflict asimetric sunt des folosite în medii academice și discursuri oficiale. „Noua strategie a celor slabi va recunoaște avantajul tehnologic, informațional și superioritatea militară a celor puternici (SUA), va evita implicarea într-un conflict direct, încercând să exploateze slăbiciunile sau să minimalizeze puterea în puncte cheie"[37].

În opinia conf. univ. dr. Ioan Bidu „în sensul semanticii, a discuta despre simetrie ar însemna să privești un ansamblu din afara lui și să-i identifici elementele componente reciproc dispuse (corespondente), realizând în acest mod o anumită armonie, concordanță și proporționalitate".

O amenințare este neconvențională tocmai datorită lipsei oricarei logici în desfășurarea ei. Ca o paradigmă, tot ceea ce este vechi trebuie dat la o parte. Astfel au judecat, posibil, teroriștii, când au transformat un obiect cu destinație civilă (avion de pasageri) în armă teroristă (atacul asupra W.T.C.)! Retoric, ne-conventionalismul nu ne mai dă voie să judecăm o acțiune de combatere a unei amenințări clasice în conformitate cu semantica conventionalismului. Modul de a lucra (acționa) conform unei obișnuințe este exclus. Până în pre-

——— [37] John. C. Gannon-Chairman, *National Intelligence Concil National Security*, in the Next Generation, www.cia.gov.

zent, „putem considera că tot ceea ce este asimetric și neconvențional, prin extrapolare devine unic"[38].

Se poate afirma că, uneori, amenințările asimetrice generează tensiuni, conflicte și crize cu consecințe imprevizibile în cadrul mediului de securitate, atât la nivel internațional, regional cât și local, un exemplu în acest sens fiind dat de derularea cu intenție a unor activități economice ce au ca rezultat deteriorarea mediului înconjurător.

Efectul încălzirii globale, creșterea nivelului mării, schimbarea centurilor climatice și instabilitatea climatică nu se constituie în amenințări directe la securitatea globală dar pot contribui probabil la riscurile unor conflicte interne sau interstatale acolo unde tensiunile sunt generate de alte rațiuni, deși efectele respective nu vor cauza direct un conflict. Cu toate acestea este probabil că încălzirea globală să sporească vulnerabilitatea acelor state fragile care nu sunt în măsură să fie buni manageri ai consecințelor schimbării. Aceasta situație poate să genereze creșterea solicitărilor militarilor la participarea în operațiuni de asistență umanitară, pentru înlăturarea efectelor dezastrelor, ce pot afecta și degrada mediul înconjurător.

Mutațiile produse în ultimul deceniu, pe plan internațional, expresii ale realităților inerente unei lumi în profundă schimbare, incumbă și modificarea sensibilă a echilibrelor strategice în regiunea sud-est europeană și conduc atât la crearea de oportunități cât și la proliferarea unor noi riscuri și amenințări — unele cu manifestări atipice în planul securității statelor din zonă.

O dată cu schimbarea configurației geopolitice a Europei și a lumii, registrul de amenințări, vulnerabilități și riscuri la adresa păcii și stabilității statelor a fost completat de:

– consecințele globalizării care mențin sau adaugă noi forme de tensiune în unele regiuni ale lumii;

---

[38] *Meridiane de securitate*, coordonator prof. univ. dr. Ioan Bidu, prefață Editura A.N.I., București, 2004, p. II.

– politicile imprevizibile promovate de unele state cu regimuri autoritariste;

– semnarea unor tratate sau acorduri ce ar putea pune în pericol interesele fundamentale ale unei țări, precum și luarea unor decizii politice de unele guverne, cu încălcarea Constituției unei țări;

– posibilitatea unor războaie inter și intra statale ce pot avea implicații negative asupra securității statelor vecine;

– apariția unor noi forme ale confruntării prin deplasarea accentului pe utilizarea forței armate și angajarea preponderentă a altor categorii de mijloace și metode, dintre care se detașează cele specifice terorismului cu toate formele sale de manifestare;

– evoluții negative în plan subregional, regional sau internațional în domeniul dezvoltării economice, democratizării, a respectării drepturilor și libertăților fundamentale ale omului, ce ar putea genera situații de criză cu efecte destabilizatoare;

– pericolul nuclear, accidentele ecologice, dezastrele naturale, nucleare, chimice sau de altă natură, ce pot pune în pericol securitatea tuturor statelor din jur, la care se adaugă efectele potențiale ale unor procese naturale la nivel global și derularea unor activități economice, care nu respectă standardele internaționale de protecție a mediului;

– limitarea accesului unui stat la sursele de energie;

– îmbogățirea ansamblului amenințărilor, riscurilor și surselor de risc cu unele forme deosebit de periculoase precum: proliferarea nucleară, contrabanda cu armament și tehnologie supusă controlului, corupția și activitățile ilegale generate de economia subterană, susținute de metode ale crimei organizate, ce erodează statul de drept, precum imigrația ilegală, traficul de persoane, arme, droguri;

– multiplicarea conflictelor etnice și exacerbarea naționalismului ce erodează conceptul de „stat națiune";

– globalizarea economică și informațională, proces care a determinat și efecte secundare negative, printre care încurajarea migrației ca o consecință a războiului etnic ori

lărgirea ariei geografice și diversificarea mijloacelor de acțiune a vectorilor amenințărilor transfrontiere ori incitarea la intoleranță, separatism, xenofobie sau extremism;

– amplificarea fenomenului de imigrare a specialiștilor din diferite domenii de vârf ale științei, tehnologiei și informaticii ce afectează potențialul de dezvoltare a unor țări;

– existența unor dificultăți de natură economico-financiară și socială generate de procesul lent de tranziție structurală internă în unele state, cu efecte asupra populației și asupra asigurării stării generale de normalitate la care se adaugă pierderea controlului statului asupra unor domenii, sectoare ori obiective economice strategice sau pierderea unor importante piețe interne sau externe pentru produsele și serviciile unei țări;

– amploarea luată de fenomenul infracționalității în unele state aflate în tranziția către o economie de piață, întârzierile de aplicare și insuficienta coordonare a reformelor în domeniul justiției și administrației publice, precum și absența unei colaborări eficiente între instituțiile cu competențe în aceste domenii;

– acțiuni individuale sau colective de accesare ilegală a sistemelor informaționale și manipulare a informațiilor cu impact asupra sistemelor de securitate ale statelor;

– menținerea unor stări de insecuritate și incertitudine socială în unele state, precum și a birocrației funcționarilor publici, cu efecte negative asupra credibilității instituțiilor, a coeziuni sociale și civice, cu impact asupra eficienței relațiilor de cooperare la nivel internațional.

– răspândirea unor maladii și viruși precum tuberculoza sau SIDA;

– deteriorarea sistemului educațional și „poluarea" morală sau culturală;

În cazul României, potrivit opiniei exprimate de Marian Rizea[39], în condițiile globalizării, pe fondul accentuării inter-

——— [39] Marian Rizea, *Riscurile asimetrice non clasice la adresa securității naționale a* României, a X-a sesiune de comunicări științifice

dependențelor și liberalizării schimburilor de orice fel cu alte state, pot fi evidențiate următoarele riscuri asimetrice, ne-clasice ce prezintă periculozitate, atât pe plan intern cât și extern:

– riscul potențial pe care îl prezintă pentru mediul înconjurător imensele rezervoare subterane de saramură reziduală situate la Ocna Mureș, Ocnele Mari și Târgu Ocna în proximitatea râurilor Mureș, Olt și respectiv Trotuș, ce pot produce prin deversarea accidentală sau intenționată de saramură o catastrofă tehnică cu efecte asupra siguranței naționale și populației, prin afectarea surselor cu apă dulce, iminența unor conflicte și litigii cu statele vecine (râurile menționate fiind afluenți direcți sau indirecți ai Dunării), afectarea florei, faunei și deteriorarea sau scoaterea din uz a stațiilor de apă potabilă;

– riscul pentru securitatea ecologică națională rezultat de acumulările de hidrocarburi gazoase în care predomină gazul metan care poate determina producerea unor explozii subterane devastatoare în numeroasele mine de cărbune și petrol închise în ultimii 14 ani, ca urmare a programelor de restructurare energetică (zona Bușteni — Telega în județul Prahova, din apropierea barajului Paltinu sau cel construit la circa 40 km N-E, respectiv la Mâneciu Prahova, ce poate afecta printr-un accident tectonic populația pe direcția Paltinu, Măneciu — Ploiești — București);

– depozitarea defectuoasă a deșeurilor rezultate din funcționarea centralelor termonucleare în condițiile în care în prezent grupurile criminale organizate și chiar teroriste sunt interesate în prelucrarea acestora cu efecte negative dificil de previzionat asupra mediului și populației prin: infestarea pânzei freatice, creșterea artificială a gradului de radioactivitate în zonele populate etc.

——— „Securitate și societate provocările mileniului trei" Secțiunea Securitate și Siguranța Națională. Amenințări asimetrice, Editura A.N.I. 2004, p. 273–281.

Unele dintre vulnerabilitățile și riscurile menționate, la nivel global, au generat creșterea ponderii misiunilor specifice operațiunilor, altele decât războiul[40], în portofoliul militar al sarcinilor repartizate militarilor, intervenții cu rol de sprijin sau ca instrument principal în funcție de amplitudinea amenințărilor și creșterea responsabilităților în domeniul contracarării amenințărilor informaționale și protecției infrastructurii naționale critice, inclusiv în spațiul digital.

În lumea posterioară *„războiului rece"* când regionalizarea constituie principala tendință a puterii și strategiei militare, se produce o proliferare a armelor, inclusiv a celor de distrugere în masă, care amenință securitatea comunității internaționale, îngrijorată tot mai mult de acumulările excesive de arme.

La sfârșitul secolului trecut, proliferarea armelor nucleare a generat o diminuare a monopolului nuclear al celor două super-puteri, SUA și Rusia, având ca efect apariția unor actori atât statali cât și ne-statali cu posibilități de producere a armamentului nuclear și a diverselor componente ale acestuia.

Tentativele și acțiunile pentru achiziționarea, deținerea, comercializarea și posibilitatea utilizării armelor de distrugere în masă de către actorii implicați în asemenea operațiuni pun în prim planul priorității politicilor de securitate ale statelor perspectiva limitării acțiunilor prin mecanisme economice, militare și de cooperare strategică.

În prezent, statele acționează pentru luarea unor măsuri de neproliferare — unilaterale, bilaterale sau multilaterale — concretizate în special în controlul exporturilor de tehnologie, echipamente, cunoștințe, bunuri strategice care ar putea fi folosite pentru producerea și dezvoltarea armelor

[40] Aceste misiuni ale militarilor care nu se înscriu în sfera tradițională a războiului vizează: menținerea și impunerea păcii, asistență umanitară, misiuni de căutare/salvare, intervenții în caz de catastrofe și dezastre civile, sprijin pentru reconstituirea structurilor statale aflate în dificultate — Bosnia-Herțegovina, Albania, Noili etc.

de distrugere în masă și a rachetelor purtătoare, care reprezintă o amenințare la adresa păcii, securității și stabilității internaționale.

Totodată statele, alături de cerințele menite să prevină amploarea înregistrată de traficul cu arme, desfășoară activități și programe active de combatere a proliferării mijloacelor de diseminare a acestora, mergând de la aplicarea tehnicilor de control specializat a exporturilor și licențelor, până la folosirea forței, strategia de reprimare axându-se însă pe o bază legală, în absența căreia nimic nu poate fi justificat.

Proliferarea armelor cu efecte de distrugere în masă și a mijloacelor de transport la țintă, va crește în special în ceea ce privește armele biologice și tehnicile asimetrice de distribuire, astfel încât statele își vor reevalua strategiile și acțiunile către o apărare națională dezvoltată combinată cu o acțiune militară activă și preventivă, atât împotriva grupurilor criminale organizate cât și a terorismului internațional.

Cu privire la noile riscuri de securitate, îndeosebi proliferarea armelor de distrugere în masă și a rachetelor purtătoare de astfel de arme, România susține obiectivul neproliferării, fiind parte la acordurile internaționale relevante și având calitate de stat membru la regimurile de control al exporturilor de produse și tehnologii cu dublă utilizare, cu excepția Regimului de Control al Tehnologiilor pentru Rachete — MTCR.

La nivel național, Agenția Națională de Control a Exporturilor (ANCEX) este răspunzătoare de aplicarea și respectarea regimului de control al exporturilor și importurilor de produse strategice.

În contextul regimurilor internaționale de neproliferare a armelor și a sistemului național de control al exporturilor și importurilor produselor și tehnologiilor cu dublă utilizare, România a luat măsuri pentru prevenirea transferului neautorizat al unor astfel de bunuri către statele supuse restricțiilor internaționale (prin controlul transferului de informații electronice între firmele supuse verificării, ana-

liza documentelor, a produselor și tehnologiilor, consultarea de specialiști,etc.).

De altfel, noul statut de membru NATO conferă României autoritatea de a gestiona cu responsabilitate riscurile și amenințările la adresa mediului de securitate euro-atlantic, sens în care țara noastră își concentrează eforturile pentru a fi un furnizor credibil și durabil de securitate regională și internațională, printr-o politică coerentă, susținută pe baza progreselor economice și sociale, prin îndeplinirea misiunilor și obiectivelor de către structurile de securitate în cooperare cu partenerii externi.

Obsesia supraviețuirii și teama de amenințările convenționale (militaro-statale) a lăsat loc, treptat, unor noi modele de cooperare și interdependență în fața unor amenințări mai *„voalate, greu de identificat și imposibil de rezolvat prin puterea militară"*.

Citând teoria lui Alexander Wendt[41], se poate constata că s-a pornit de la o „cultură" a anarhiei de tip *„lockeari"* (actori rivali care își recunosc reciproc suveranitatea și nu își amenință direct existența) și s-a ajuns, actualmente în zona unei *„culturi kantiene"* (relații de prietenie, încredere reciprocă, evitarea conflictelor acute și solidaritatea în fața pericolelor exterioare).

Lumea relațiilor internaționale, adică a interacțiunilor dintre statele suverane a arătat că mediul de securitate, provocările și răspunsurile sunt dinamice, în condițiile apariției unor noi riscuri și amenințări la adresa comunității internaționale.

În prezent se constată o amplificare și o a lărgire a spectrului de riscuri neconvenționale, diversitatea tipologiei crizelor și conflictelor care generează provocări numeroase, necesitând reacții multidirecționale bazate pe mobilitate, diver-

[41] Standley Hoffmann, *Sisiful european" Studii despre Europa (1964–1994)*, trad. românească Elena Neculce, Cartea veche, București 2003, p. 411–417.

sitate, coerență și complementaritate atât în spațiul intern cât și în cel internațional.

Totodată, periculozitatea entităților ce generează/favorizează riscuri și amenințări de această natură este maximizată prin efectul caracteristicilor comune: subversitatea (activitatea lor este îndreptățită, explicit sau implicit, împotriva ordinii de drept și a stabilității sociale dintr-unul sau mai multe state); dimensiunea transnațională (obiectivele urmărite le impun strategii transfrontaliere); secretizarea (structurile respective au o organizare și funcționare discrete, clandestine, cel puțin în fazele incipiente ale dezvoltării lor)[42].

CRIMINALITATEA STRATEGICĂ

Crima organizată și terorismul reprezintă amenințări asimetrice pentru securitatea comunității internaționale, ce nu trebuie privite separat ci într-o profundă interacțiune dată de natura fluctuantă a ambelor fenomene transnaționale, de utilizarea unor metode și tactici violente, de realizare a obiectivelor propuse (chiar dacă motivațiile sunt diferite) de implicare în afaceri criminale dar și semilegale, pentru camuflarea acțiunilor ilicite și de spălare a banilor, activități planificate de structuri organizate, piramidale ce au la bază reglementări rigide și oculte de aderare, protecție și sancțiune a membrilor.

În prezent, se poate vorbi de o criminalitate strategică ce reprezintă o combinație letală între crimă organizată și terorism, ce urmărește uzurparea puterii politice, prin crearea unei economii paralele care deteriorează credibilitatea instituțiilor fundamentale ale statului de drept în fața cetățenilor, ce se confruntă cu o lezare a drepturilor și libertăților

[42] Centrul de Studii și Cercetări pentru Siguranța Națională, *Reforma Serviciului Român de Informații*, coordonator Alexandru Radu Timofte, București 2003, p. 36–38.

fundamentale dar și cu riscurile provocate de infracționalitatea transfrontalieră atât la nivelul securității individuale, cât și ale comunității în general.

Această criminalitate rezultată din simbioza dintre terorism și crima organizată cu cel mai nociv rezultat — narco-terorismul — amenință viața și proprietatea cetățenilor, dar în același timp corupe și distorsionează activitatea instituțiilor democratice, vulnerabile în perioada de tranziție spre economia de piață.

Crima organizată, la fel ca și terorismul, nu reprezintă o realitate specifică regimurilor post-comuniste, rădăcinile acestora și seva activităților criminale ce au înregistrat niveluri din ce în ce mai sofisticate de organizare și perfecționare, în concordanță cu tehnologiile moderne, se găsesc și se întrepătrund cu iraționalitatea economiei ultra-centralizate și a vastei „piețe negre", ce a germinat în ultimele două decade ale regimului comunist.

„Piața neagră" a avut un rol important în inocularea în societate a tradițiilor pieței libere, dar ceea ce a fost cel mai ușor de învățat au fost modalitățile insidioase de eludare a legii. În același mod în care piața neagră a înflorit acolo unde prezența statului nu a fost precumpănitoare, grupurile criminale au exploatat situațiile în care autoritatea și resursele statului erau slăbite, deci vulnerabile la subversiune.

Noile sisteme politice și noile realități economico-sociale sunt oportunități abil valorificate de infractori, indiferent dacă aparțin grupurilor criminale organizate sau organizațiilor teroriste. În condițiile prăbușirii nivelului de trai al cetățenilor debusolați, din țările foste comuniste, care s-au angrenat în activități economice muribunde, datorită tranziției, tentația acestora de a obține profituri ușor de dobândit a fost materializată și în adeziunea la activități criminale organizate.

A apărut astfel o conjugare de factori de destabilizare și de amenințare a securității țărilor încadrate în „noile democrații", principalii actori de subminare a progresului fiind violența de tip insurgent și criminalitatea endemică.

În acest context, deschiderea frontierelor, libertatea de exprimare, economia de piață reprezintă un teren fertil pentru terorismul ce tinde în prezent să stabilească o relație fructuoasă cu crima organizată și în special, cu formele cele mai violente de manifestare a acesteia — traficul de droguri și armament — la care se adaugă interferența cu conflicte de mică intensitate, concentrate la nivel etnic, anarhic și integrism religios, specifice unor state precum Ruanda, Liban, Columbia, Sri-Lanka.

Noile realități și relații economice, disoluția comunismului, a Uniunii Sovietice și a Pactului de la Varșovia au accentuat procesul de „ghetoizare" a aglomerațiilor urbane, apariția conflictelor între bande, grupuri organizate pentru împărțirea zonelor de influență sau protecție, precum și alienarea unor minorități sociale, religioase paralel cu amploarea militantismului extremist și polarizarea rasială.

În plan intern, democrațiile emergente au fost confruntate cu o triplă transformare produsă în paralel: trecerea de la o economie comandată central la o economie liberă de piață, transformarea politicii antiteroriste într-una liberală și renunțarea la securitatea centralizată, în ideea conturării unui sistem național independent de apărare a siguranței naționale.

Procesele rapide de liberalizare și democratizare au surprins nepregătite noile guverne care nu se puteau baza pe structurile rigide polițienești și de securitate, ce sufereau de mentalități învechite și birocratizări excesive și nu concepeau decât metode inflexibile și represive de acțiune împotriva valului infracționalității. Grupurile criminale organizate și teroriste au exploatat facilitățile oferite de tensiunile și sincopele inerente proceselor complexe de transformare, survenite în societate și s-au extins transfrontalier.

Schimbările regimurilor politice au produs restructurări masive, epurări ale personalului suspectat de afilieri politice, reorganizări succesive pe criterii de imagine, schimbarea competențelor și a manierelor acționale, toate acestea diminuând pe termen scurt și mediu eficacitatea structurilor și

instituțiilor abilitate să asigure ordinea publică și siguranța națională.

Structurile societății civile, administrației și infrastructura economică a țărilor est-europene s-au dezvoltat lent, ilegal și inconsecvent, față de noi parametri ceruți de economia concurențială, rigorile globalizării economiei mondiale și noile curente politice. Adaptabile la schimbări, atât crima organizată cât și terorismul, în mod spectaculos, au prosperat, câștigând teren și resurse financiare uriașe, prin influențarea zonei economice, sociale și politice, unde prin corupție, șantaj, amenințare și chiar violență și-au consolidat sistemic viabilitatea structurilor.

Din aceste motive, multe dintre măsurile preconizate de statele aflate în perioada de tranziție au eșuat lamentabil în fața capacității de supraviețuire a criminalității strategice, care a început să controleze sistemic diferite domenii ale afacerilor legale.

Legătura organică dintre crima organizată și terorism din punct de vedere statistic este relevată și de modalitățile de acțiune infracțională. Astfel, 47,9% presupun violență fizică și intimidare, iar 16,2% se concretizează în influențarea politicienilor, mijloacelor de comunicare în masă, publicului și reprezentanților sistemului judiciar ori administrativ.

Nici terorismul nu s-a lăsat mai prejos, iar perfidele și evoluatele forme de manifestare au zdruncinat intens temelia fragilă a statelor democratice în formare.

Deși mulți specialiști au considerat terorismul ca un fenomen în declin, totuși, acest fenomen, prezent permanent pe scena politică internațională și-a modificat și rafinat strategiile de acțiune în scopul obținerii unor obiective mai mari prin focalizarea activităților teroriste pe ținte reduse ca număr dar simbolice, prin efectele dezastroase și propagarea exponențială a sentimentelor de groază, panică, neliniște ce cutremură sensibilitatea comunității (ex. atentatele teroriste din SUA din 11 septembrie 2001).

Terorismul contemporan se bucură de o senzațională atenție, la fel ca și grupurile de crimă organizată (când reușesc să surprindă publicul prin șocante infracțiuni de violență ori trafic de droguri, armament sau ființe umane), ambele necesitând „tratamente" juridice adecvate gradului de pericol social concret și consecințelor survenite la nivelul echilibrului social, economic și politic.

Angajate în lupta împotriva crimei organizate și terorismului, autoritățile statului trebuie să acopere un număr mare de domenii afectate de infracționalitatea în continuă expansiune, să depășească barierele de implementare a sistemului normativ și mai ales să țină cont de respectarea drepturilor și libertăților fundamentale ale cetățenilor. Totodată, guvernele se confruntă în acțiunile de prevenire și combatere a activităților criminale cu un grav paradox produs de globalizare: capacitatea grupurilor organizate de a exploata deschiderea frontierelor, la care se adaugă continua perfecționare a acțiunilor ilicite în pas cu ultimele cuceriri ale tehnologiei informaționale.

Într-o societate democratică, avantajul inițial este probabil de a conviețui cu teroriștii. În particular, există limite cu privire la ceea ce se poate face pentru a preveni și contracara atentatele care sunt concepute și lansate din exterior.

Principalele obiective ale statelor, prin organele abilitate, vizează erodarea capacității grupurilor teroriste și celor aparținând crimei organizate, de a săvârși acțiuni ori atentate, prin obținerea de informații despre componența, infrastructura și metodele acestora, folosirea acelor informații care permit evaluări ale amenințării în luarea de măsuri adecvate de protecție, distrugerea fondurilor, a armelor, tehnologiei și echipamentelor de care acestea uzează, subminarea dorinței infractorilor de a continua violența, furnizând în același timp organelor judiciare suportul adecvat pentru tragerea la răspundere penală a acestora.

Grupările teroriste au înțeles și ele că distrugerea infrastructurilor informaționale și periclitarea vastelor rețele,

constituie un mijloc de presiune la fel de periculos ca depunerea de bombe în locurile publice.

Cyberterorismul va fi arma celor puternici, tehnologia va deveni arma supremă, veritabila armă globală, tehnicile războiului informatic fiind la îndemâna statelor, organizațiilor teroriste și nu în ultimul rând a grupurilor criminale organizate.

Globalizarea implică și reprofesionalizarea atât a crimei organizate cât și a terorismului. Rețelele se folosesc de ultimele cuceriri în materie de tehnologie și comerț pentru a-și extinde și perfecționa activitățile ilegale, dovedind o maximă eficiență și dispunând de resursele financiare necesare pentru a garanta orice tip de acces la tehnologia modernă de care au nevoie. Acestea nu se rezumă doar la informatică, ci includ în egală măsură telecomunicațiile și tot ceea ce conține o valoare materială. „Este clar că în prezent, criminalitatea organizată e în măsură să utilizeze cu eficiență cele mai moderne mijloace tehnologice de gestionare economică", afirma Jean Claude Monet, comisar al Poliției franceze[43].

Terorismul și crima organizată vor converge din ce în ce mai mult, organizațiile criminale fiind utilizatori avizați ai noutăților tehnologice, care le oferă posibilitatea de a se sustrage anchetelor și tuturor investigațiilor efectuate de organele abilitate. Utilizând computerele, membrii acestor rețele criminale obțin, protejează și procesează informațiile de care au nevoie pentru a deruta anchetatorii. În plus, această tehnologie le permite să elaboreze strategii de introducere a drogurilor, armelor sau a altor mărfuri de contrabandă pe piață, să stabilească rețelele și metodele cele mai eficiente de a le transporta și de a încheia tranzacții financiare, punând totodată autoritățile pe o pistă falsă.

Pe de altă parte, aceste rețele profită de ritmul accelerat și de numărul mare al tranzacțiilor financiare, precum și de faptul că există foarte puține măsuri de prevenire a abu-

[43] *Criminalite Organisee*. INESI, doc. franc., 1996, p. 8.

zurilor, sistemul permițând transferul unor sume foarte mari fără supraveghere strictă, astfel încât spălarea banilor rezultați din infracțiuni devine posibilă, iar confiscarea acestora potrivit reglementărilor în vigoare, este dificil de realizat.

În timp ce războiul cybernetic — concept care se referă la războiul militar împotriva informațiilor — aduce în arenă, de obicei forțe militare, una împotriva alteia, este mai probabil ca războiul în rețea să implice forțe neguvernamentale, paramilitare și neregulate ca în cazul terorismului și crimei organizate.

Crima organizată este interesată de tehnici rezervate strategiilor ofensive, gândite în scopuri militare din două motive. Primul rezultă dintr-o rețea de operare contra unei amenințări și acțiuni represive din partea organelor judiciare, al doilea motiv este legat de un calcul simplu, raportul calitate-preț este foarte avantajos.

Recrutarea câtorva „hackeri" foarte încântați de a avea în sfârșit ocazia să-și pună în valoare performanțele, istețimea și abilitatea dobândită prin accesul neautorizat la sistemele informatice, nu reprezintă decât o cheltuială minimă în raport cu posibilele beneficii.

Mai îngrijorător este faptul că unele organizații criminale și teroriste, folosesc noua tehnologie pentru a detecta activitățile desfășurate de agențiile de aplicare a legii. Faptul că aceste organizații criminale dispun de fonduri uriașe destinate achiziționării de tehnologie sofisticată, pune în inferioritate forțele de aplicare a legii de securitate, care nu sunt dotate corespunzător, mai ales în statele care se confruntă cu o creștere a ratei infracționalității de tip criminal organizat, dificil de controlat și anihilat.

Echipamentul performant de care dispun, oferă grupurilor organizate sau teroriste, posibilitatea de a realiza vendete sau de a lua drept ținte, înalte oficialități de pe scena politică, juridică sau din cadrul guvernului, dacă interesele le sunt amenințate. Motivația este diferită însă, grupurile teroriste fiind animate de susțineri și revendicări politice,

rasiale, teritoriale, „care în ciuda folosirii celor mai moderne tehnici, se inspiră din miturile profund arhaice"[44]

În același timp, noua tehnologie, cu evoluția ei rapidă și radicală, pune o mulțime de probleme de ordin politic, socio-economic și juridic, așa cum se constată din ce în ce mai des în ultimul timp, în urma săvârșirii unor acțiuni ilegale cu caracter inedit și transfrontalier. Dacă până nu demult se vorbea numai de pirateria software și despre epidemiile de viruși informatici, acum, în contextul extinderii rețelelor interactive și deschise de informație, activitatea ilegală informatică este cu mult mai periculoasă, afectând întreg spațiul virtual.

O diferență între grupurile criminale organizate și organizațiile teroriste rezidă și din elementele care determină aprecierea existenței unei astfel de asociații. Grupurile crimei organizate se delimitează atât de grupurile de indivizi care se asociază relativ întâmplător și desfășoară o activitate infracțională de amploare redusă sau ocazională cât și de acțiunile ilicite ale unui individ chiar dacă prezintă o motivație similară cu a unei asociații criminale.

Pentru a ne afla în prezența unui grup criminal organizat trebuie ca acesta să fie format din cel puțin trei persoane, să prezinte o structură clandestină ermetică, organizatorică de tip ierarhic, cu o ideologie comună și cu ritualuri de aderare și o ierarhie piramidală de conducere ce propagă o disciplină severă cu sancțiuni severe în caz de încălcare a secretului operațiunilor. Activitățile se desfășoară sistematizat și planificat într-o perioadă lungă de timp sau nedefinită în scopul obținerii, în mod direct sau indirect, de profit financiar, material și/sau putere ori a unor avantaje morale pentru a controla și influența prin metode ilegale (cum ar fi violența, amenințarea cu violența, intimidarea, teroarea, corupția, șantajul, accesul neautorizat la sistemele informatice, pretinderea taxelor de protecție, traficul de

[44] Norman Cohn, *Les fanatiques de l'Apocalypse*, p. 295, citat de Jean Servier, *op.cit.*, p. 41.

influență...) instituții publice, autorități, persoane de interes public ori privat care le pot facilita atingerea obiectivelor, dobândirea și menținerea prestigiului aparenței de respectabilitate a grupului.

Grupurile criminale organizate acționează la nivel național și internațional, în sistem de tip rețea, membrii acestora fiind suspectați de comiterea unor infracțiuni grave pasibile de o pedeapsă privativă de libertate al cărei maximum nu trebuie să fie mai mic de patru ani sau de o pedeapsă mai grea. Prin acțiunile lor, aceste grupuri, ce au la bază legături stabile de asociere și continuitate a operațiunilor (nefiind excluse nici acordurile sporadice pentru atingerea scopurilor sau valorificarea oportunităților), pot aduce atingere sănătății populației, mediului, ordinei de drept și chiar siguranței naționale a unui stat.

Aceste asociații criminale organizate recurg la practici ilicite în tranzacțiile internaționale, comerciale, la tehnici de spălare a banilor pentru reinserția capitalurilor și majorarea cuantumului profiturilor și valorificarea legislației privind secretul bancar, lacunele legislative din diferite domenii, neplata taxelor, instituirea monopolului asupra unor produse, infiltrarea în afaceri legale și influențarea derulării activității acestora, înființarea de întreprinderi ilegale, achiziționarea ilegală de capital, exercitarea controlului asupra unor activități economico-sociale etc.

În ceea ce privește terorismul, acesta a devenit accesibil oricărei persoane care are o nemulțumire, un plan, un scop sau o combinație a tuturor acestor motivații, nefiind doar apanajul grupurilor teroriste organizate. Pe baza manualelor sau îndrumătoarelor care se găsesc în comerț despre fabricarea bombelor, teroristul amator poate fi la fel de periculos și chiar mai dificil de identificat, decât teroristul de profesie. Teroriștii amatori își pot alătura uneori acțiunile, la motivația și îndeplinirea obiectivelor teroriste ale unei rețele profesioniste, fiind astfel mult mai periculoși. Absența unei autorități centrale de comandă înseamnă mai puține constrângeri pentru teroriștii amatori, în alegerea țintelor și

modalitatea de executare a operațiunilor, mai puține inhibiții în ceea ce privește victimele, mai ales când există motive religioase, ceea ce duce la săvârșirea unor acte deosebit de violente și spectaculoase, în scopul captării atenției mass-mediei și a cuceririi unei celebrități temporare.

Terorismul motivat total sau parțial de imperative religioase a dus adeseori la acte mult mai dramatice, cu o intensitate a violenței, a instaurării terorii și a producerii unui număr mai mare de victime, decât terorismul laic.

Acest lucru poate fi explicat prin prisma sistemelor de valori radical diferite, a mecanismelor de legitimare și justificare a conceptelor moralității, care afectează direct „motivația terorismului sfânt". Pentru teroristul religios, violența este un act sacru sau o datorie divină, executat direct din ordine teologice și justificate de scriptură. De aceea, religia funcționează ca o forță de legitimizare, sancționând în mod special violența pe scară largă împotriva unei categorii nelimitate de opozanți (de exemplu oameni care nu aparțin religiei sau cultului teroriștilor).

O similitudine cu domeniul de manifestare a crimei organizate poate fi avută în vedere dacă ne raportăm din punct de vedere al motivației religioase la sectele generatoare de crime, care sunt grupuri de oameni legați prin pseudo-ritualuri care împart și cred în același sistem de valori (în mod obișnuit elaborat de grup, pe baza unui fundament religios) și desfășoară activități contrare legii.

Sectele, spre deosebire de grupurile organizate criminale sau grupurile teroriste, au o structură ierarhică rigidă, în care membrii sunt legați între ei prin legături de ordin psihic, care pe baza unor ritualuri de „frăție de sânge", aderă la regulile grupului religios, acceptă sistemul sancționator rigid precum și ideologia inoculată prin utilizarea unor tehnici de psiho-manipulare contrare eticii, ce pot duce la tulburări de personalitate, sinucideri în masă și alienări ale comportamentului social.

Dacă secta este orientată spre o activitate criminală atunci crimele, în raport cu doctrina culturală, se vor con-

cretiza în crime abominabile, însoțite de violuri și atrocități comise asupra corpurilor victimelor ori ale animalelor, oferite în semn de ofrandă divinității, în conformitate cu sacrificiile comandate.

Înțelegerea și întreruperea legăturilor de finanțare a crimei organizate, în special cea reprezentată de organizațiile criminale implicate în traficul de arme și droguri, care cooperează cu teroriștii, vor pune capăt unei surse importante de sprijin pentru unele dintre cele mai violente grupări teroriste, motivate politic, astfel încât comerțul cu tehnologiile letale scumpe vor fi din ce în ce mai greu de procurat de infractori și în același timp, eficient controlate de autorități.

Logistica activității desfășurate de grupurile criminale organizate, precum și a organizațiilor teroriste este asigurată printr-un complex de măsuri și acțiuni derulate într-o manieră sistemică, descentralizată, conspirată, autonomă sau în conexiune cu alte asociații similare, uneori beneficiind și de ajutorul unor state sau organizații neguvernamentale. Mijloacele financiare obținute de aceste grupări criminale sunt necesare procurării, cercetării și realizării suportului realizării activităților ilicite, pregătirii și antrenării membrilor grupului, asigurării mijloacelor tehnice, de telecomunicații, transport, asistență medicală și a altor servicii necesare pentru atingerea obiectivelor propuse.

Întrepătrunderea activităților crimei organizate cu acțiunile teroriste ale organizațiilor de profil și diminuarea sponsorizării statale a acestora i-a determinat pe liderii celor două tipuri de organizare funcțională să-și unească tacticile și să apeleze chiar la o gamă variată de practici generatoare de resurse financiare, inclusiv prin infiltrarea într-o paletă diversă de afaceri legale și cvasilegale.

Au apărut ingenioase strângeri de donații în scop aparent caritabil sau nenumărate scheme criminale și adevărate inginerii financiar-bancare, derulate în special, în statele mai vulnerabile, aflate în procesul de tranziție, unde se puteau valorifica nu numai lacunele legislative dar și mecanismele

financiar-bancare în formare, paralel cu ineficiența unor instrumente juridice sau operaționale de represiune, din partea unor state puternic afectate de crize economico-sociale și politice.

Pe măsură ce motivațiile teroriste au început să se îmbine tot mai armonios cu motivațiile grupurilor criminale organizate și să aibă interese comune, inclusiv în zona procurării resurselor financiare, ascunderea originii ilicite a acestora și legalitatea unor activități derulate în economia la vedere, în aceeași măsură statele, conștiente de noile amenințări transnaționale, au intensificat cooperarea în domeniul prevenirii și contracarării activității acestor „actori" care pe scena mondială joacă diferite roluri, multe din ele provocând „în direct" comunității, șocante sentimente din care nu lipsesc groaza, frica, oroarea și teama, inoculate la intensitate maximă.

În prezent, liniștea și siguranța fiecărui cetățean nu mai pot fi disociate de cele ale comunității și nu pot fi privite decât în contextul siguranței naționale a unui stat. Problema la ordinea zilei este a conștientizării pericolului real reprezentat de infracționalitate (indiferent dacă se referă la violența de la nivelul crimei organizate sau cea specifică terorismului), aspecte care determină schimbări în abordarea strategică a provocărilor și amenințărilor conturate la adresa siguranței naționale.

În lupta împotriva crimei organizate și a terorismului, organele de aplicare a legii trebuie să coopereze cu serviciile naționale de informații, astfel încât, prin împletirea eforturilor acestora, să se realizeze o combinație eficientă de metode investigative, care să garanteze maximum de rezultate într-o perioadă scurtă de timp și să minimalizeze riscurile deconspirării investigatorilor sau a metodelor secrete folosite ori al imixtiunii în viața privată a suspectului, a familiei sau persoanelor din anturajul acestuia.

Se constată totodată și o abilitate deosebita a teroriștilor și a membrilor grupurilor criminale organizate de a eluda legea și de a se sustrage de la urmărire și judecată prin

manipularea mecanismelor justiției, prin șantaj, violență, corupție, câștigând astfel influență și stabilitate în zona în care operează.

În aceste condiții, statele confruntate cu provocările, amenințările și efectele operațiunilor teroriste și ale grupurilor criminale organizate își reorientează politicile de protecție și pun în practică instrumente juridice și forțe de acțiune ale personalului abilitat, să prevină și să contracareze asemenea forme de manifestare a infracționalității.

În acest nou „război", declanșat între forțele de ordine și inamicii misterioși, concentrați pentru a da eficiență acțiunilor, în grupuri mici, descentralizate dar cu răspândire transfrontalieră, se impune revizuirea mentalității de abordare a pericolului pentru siguranța națională a statelor și punerea în practică a strategiilor adecvate de combatere, paralel cu dotarea „oamenilor legii" la un nivel tehnologic performant.

Se are în vedere nu numai reforma sistemului justiției dar și reorganizarea forțelor polițienești și a serviciilor de informații, pentru asigurarea ordinii și liniștii publice pe termen lung, soluționarea tuturor conflictelor apărute încă în stadiile incipiente, asigurarea ordinii de drept și protejarea securității naționale.

Guvernele trebuie să adopte maniere inovatoare de abordare a amenințărilor crimei organizate și terorismului, atât prin mijloace și instrumente aplicate la nivel național, dar și prin întărirea cooperării internaționale, pentru a face „front global" de contracarare a infracționalității.

Pentru a face față amenințărilor, la adresa stabilității internaționale, generate de infracționalitatea actuală și diversele ei forme de manifestare, sarcina prioritară care revine autorităților este cunoașterea și înțelegerea relațiilor complexe și misterioase existente între terorism și crima organizată, modul complex de acțiune al membrilor acestor grupări din ce în ce mai specializate, strategiile combinate folosite de infractori la nivel național și internațional, desco-

perirea vulnerabilităților și valorificarea acestora în activitățile de prevenire și combatere.

Se impune îmbinarea instrumentelor juridice de acțiune împotriva terorismului și crimei organizate deoarece, concentrarea atenției cu prioritate asupra terorismului poate crea fisuri în combaterea altor forme de infracționalitate. Mai mult, trebuie să se țină cont de interacțiunea fenomenelor și de necesitatea contracarării rapide a acestora. Practica a demonstrat că pentru capturarea teroriștilor și deferirea acestora justiției, e nevoie de mai mult timp, dar reținerea și investigarea acestora pentru alte activități criminale (decât conspirațiile sau atentatele teroriste) este mai ușor de făcut.

Al Capone nu a fost capturat pentru implicarea în activități specifice crimei organizate ci pentru evaziune fiscală și neplata contribuției la impozite, ceea ce i-a atras o sancțiune de 11 ani închisoare, care i-a terminat cariera criminală.

În „războiul" cu teroriștii și crima organizată, guvernele trebuie astfel să se mobilizeze și să acționeze cu mijloace și instrumente juridice și logistice moderne, pentru a aborda sistemic și a combate strategic, inclusiv prin metode neconvenționale și inovatoare infracționalitatea în continuă extindere pe toate meridianele lumii.

Sesizând pericolul social reprezentat de crima organizată și terorism, organismele guvernamentale și neguvernamentale și-au dat mâna la cel mai înalt nivel pentru identificarea și punerea în practică a celor mai eficiente căi și mijloace de contracarare a acestor fenomene.

ONU și organizațiile mondiale și regionale competente trebuie să ajute statele să pună la punct modele și directive practice în materie de drept penal și drept procesual penal, să examineze și să evalueze legislația în domeniu, să planifice și să întreprindă reforme ținând cont de realitățile, specificul și tradițiile culturale, juridice și sociale existente în fiecare țară și să intensifice activitatea instituțiilor de cooperare internațională.

Legiuitorii din fiecare țară trebuie să țină pasul cu organizațiile criminale care-și modifică permanent metodele, invadează noi domenii de activitate și valorifică inovațiile majore, cum ar fi Internetul sau serviciile financiare electronice ori consecințele liberalizării deplasării persoanelor și exploatează libera circulație a bunurilor și finanțelor pentru asigurarea transferului și spălării profiturilor obținute ilegal.

În vederea armonizării legislației, pentru o mai strânsă cooperare și pentru dezvoltarea mecanismelor internaționale necesare luptei contra crimei organizate, parlamentele naționale trebuie să cunoască sistemele legislative din alte state, să se alinieze schimbărilor tehnologice și modalităților utilizate în acest sens de grupurile criminale, să ia măsuri pentru conștientizarea publicului în legătură cu pericolul crimei organizate, pentru contracararea conspirațiilor împotriva autorităților de stat sau libertăților cetățenilor și să găsească cele mai adecvate instrumente de contracarare a fenomenului.

Pentru autoritățile din fiecare țară, dificultățile substanțiale în prevenirea și combaterea terorismului și crimei organizate constau, printre altele, în existența barierelor lingvistice și sociale, acoperirea unor vaste domenii de acțiune (economic, financiar, juridic etc.), capacitatea grupurilor criminale de a exploata deschiderea frontierelor, mobilitatea și structurarea acestora după strategii și tactici militare cu legături în continuă perfecționare la nivel internațional, precum și dotarea infractorilor în pas cu cele mai noi cuceriri ale revoluției tehnologiei informaționale.

Comunitatea internațională trebuie să se pună de acord asupra unei definiții comune a conceptului de crimă organizată și terorism, pentru omogenizarea măsurilor luate la nivel național și eficientizarea cooperării internaționale.

Pentru combaterea efectivă a fenomenului, statele trebuie să țină cont de caracteristicile acestui flagel, în vederea elaborării de strategii, politici, legi sau alte măsuri adecvate, valorificând în același timp experiența statelor care s-au confruntat cu crima organizată, pentru a asigura justiției

un suport corespunzător de norme, structuri și mijloace necesare derulării cercetărilor și judecării infractorilor.

TERORISMUL — AMENINȚARE LA SECURITATEA GLOBALĂ

Dezastrele provocate în mod intenționat prin acțiuni teroriste, constituie cele mai noi provocări la adresa siguranței naționale, terorismul global fiind epifenomenul cel mai expresiv al globalizării, ilustrat tragic prin evenimentele de la 11 septembrie 2001 din SUA și recent din 11 martie 2004 de la Madrid. Ele sunt considerate atacuri asimetrice neclasice și constau în acțiuni ne-armate deliberate, având ca obiective cu consecințe directe inducerea panicii, groazei în vederea obținerii unor revendicări politice, iar printre obiectivele cu consecințe indirecte se numără distrugerile materiale, slăbirea potențialului economic, a credibilității politicilor de guvernare etc.

Confirmarea responsabilității rețelei Al Qaeda în comiterea masacrului de la Madrid soldat cu 200 de morți i-a determinat pe experții în terorism să recunoască ineficiența campaniei internaționale duse până acum împotriva terorismului, factorii de decizie mobilizându-se mai ferm în relansarea cooperării europene antiteroriste.

Prof. univ. dr. Cristian Troncotă apreciază că unii analiști au pus eșecurile înregistrate în lupta împotriva terorismului pe seama perspectivei democrațiilor occidentale de abordare a terorismului, care continuă să rămână mai degrabă pasivă decât proactivă. Ei au criticat tendința guvernelor de adăugare a noi nivele de birocrație în interiorul instituțiilor implicate în combaterea terorismului după 11 septembrie 2001, în loc de a căuta să le elimine pentru a obține o mai mare eficiență în combaterea fenomenului. Birocrației sporite i se adaugă rivalitățile manifestate între diferitele

agenții de informații pentru a se afirma în operațiunile contrateroriste.

Altfel spus, decenii întregi de cultură specifică „războiului rece" și de birocratizare vor trebui uitate, iar specialiștii susțin că schimbările în planul mentalităților se produc mult mai greu decât cele din planul organizatoric sau normativ.

Cert este că 11 septembrie 2001 a marcat sfârșitul unei epoci și începutul alteia nu doar pentru comunitatea informativă a Statelor Unite ci pentru serviciile de informații din întreaga lume[45].

Un exemplu concludent în acest sens îl constituie desfășurarea la 19 martie 2004 a Consiliului Extraordinar J.A.I .dedicat combaterii terorismului, urmat de summitul de la Bruxelles, organizat în perioada 22–23 martie 2004, la nivelul miniștrilor de externe din Uniunea Europeană ce au finalizat proiectul de declarație finală, dedicată impulsionării demersurilor contrateroriste.

Miniștrii de interne și justiție ai statelor membre U.E. și în curs de aderare au dezbătut și adoptat un set de propuneri, de măsuri specifice ce au fost supuse aprobării Consiliului European de la Bruxelles, reunit în perioada 25–26 martie 2004. În acest sens s-a decis luarea unor măsuri ferme de anihilare a terorismului internațional, ce sprijină terorismul intern sau confruntări politice, ideologice sau religioase, prin:

– limitarea accesului teroriștilor la sursele de finanțare și identificarea deținătorilor, destinatarilor și beneficiarilor conturilor de finanțare a actelor teroriste;

– depistarea, prevenirea atentatelor și destructurarea rețelelor și grupurilor teroriste;

– diminuarea și înlăturarea condițiilor și factorilor care facilitează atât sprijinul cât și recrutarea noilor membri sau

[45] Cristian Troncotă, Horațiu Blidaru, *Careul de aşi. Serviciile secrete ale Marii Britanii, S.U.A., Rusiei, Israielului*. Editura Elion, București, 2003, p. 139, 149–150.

simpatizanți ai teroriștilor, un rol important în îndeplinirea acestor obiective revenind societății civile și mass-mediei;

– punerea în aplicare sau consolidarea instrumentelor juridice existente la nivel european și internațional alături de îmbunătățirea activității tuturor componentelor și structurilor specializate de securitate care trebuie să acționeze mai ferm și să coopereze mai eficient, inclusiv în derularea schimbului de informații;

– asigurarea unui control riguros al frontierelor, inclusiv prin introducerea monitorizării electronice a datelor de identificare a persoanelor.

Măsurile concrete contrateroriste ce au făcut obiectul dezbaterilor menționate (printre care și adoptarea *„clauzei de solidaritate"*)[46] sunt menite să aplice strategia europeană de securitate, în primul rând a componentei de combatere a terorismului pornind de la cauzele care-l generează și în doilea rând pentru eficientizarea Planului de acțiune pentru combaterea terorismului adoptat în 2001.

Nu ar fi lipsit de interes, însă, preluarea în spațiul european a modelului Legii „Patriot", adoptată de Congresul SUA la 25 octombrie 2001, de introducere a elementelor biometrice de identificare a persoanelor în documentele de identitate și crearea unei baze de date cu regim special de acces.

Șocul produs de atacurile teroriste din 11 septembrie 2001, executate asupra unor obiective din SUA, precum și evoluțiile asociate campaniei antiteroriste internaționale au determinat nu numai modificări ale legislației americane, dar și:

– reevaluarea periculozității fenomenului terorist în planul stabilității și securității internaționale în condițiile convergenței cu crima organizată;

– reconfigurarea raporturilor dintre state și organizații;

---

[46] *Atentatele pun Europa în mișcare* în „Evenimentul zilei" nr. 3683, din 25 martie 2004, p. 11.

– reconsiderarea priorităților și mecanismelor de securitate ale statelor, precum și a dinamicii organizațiilor politico-militare și politico- economice internaționale;

– izolarea pe scena mondială și sancționarea mult mai severă a statelor care sprijină financiar sau favorizează terorismul, respectiv, marginalizarea celor care nu contribuie la eforturile comunității internaționale de prevenire și combatere a fenomenului[47].

USA Patriot Act (Uniting and Strenghthening of America by Providing Appropriate Tools Required to Interpret and Obstruct Terrorism) este un act normativ de referință pentru sistemul legislativ american modificat după atentatele teroriste din 11 septembrie 2001.

Legea „Patriot" reglementează printre altele interceptarea convorbirilor telefonice și ținerea sub observație a imigranților considerați suspecți.

Demne de menționat sunt următoarele prevederi ale acestei legi:

– autorizarea ascultării pe scară largă a telefoanelor, inclusiv a celor mobile, a mesajelor scrise sau vocale, pentru ca instituțiile cu atribuții în domeniu să poată cunoaște conținutul convorbirilor efectuate de o persoană suspectată de săvârșirea unor acte de terorism, fără a fi necesară, ca în cazul legislației precedente, o autorizație specială dată de organele abilitate pentru fiecare număr de telefon în parte;

– ridicarea parțială a restricțiilor privind schimbul de informații între instituțiile cu atribuții de combatere a terorismului, cu privire la persoanele suspecte de comiterea unor astfel de acte;

– stabilirea unor pedepse mai severe pentru cei care adăpostesc, protejează, găzduiesc sau facilitează activitățile teroriștilor sau cele care au ca obiect spălarea banilor sau deplasarea sumelor prin intermediul unor operațiuni financiare sofisticate între bănci;

[47] Monica Șerbănescu, Ilie Botoș, Dumitru Zamfir, *op. cit*, p. 88.

– impunerea obligației ce revine băncilor americane, de a păstra o evidență exactă a informațiilor despre clienții străini și a interdicției de a avea legături cu instituții bancare din străinătate, despre care nu au date și informații suficiente, referitoare la credibilitatea și corectitudinea operațiunilor și tranzacțiilor pe care le întreprind;

– stabilirea, în favoarea autorităților federale, a posibilității de a reține pe o durată de până la șapte zile pe cetățenii străini asupra cărora planează suspiciuni de comitere sau pregătire a unor atacuri teroriste;

– autorizarea instituțiilor specializate de a supraveghea și intercepta corespondența pe e-mail, precum și a paginilor web accesate de persoanele suspectate de comiterea sau pregătirea unor acțiuni ilicite de natură teroristă, prin monitorizarea Internet-ului.

Legea „Patriot" a înlăturat barierele care împiedicau schimbul de informații dintre serviciile de informații și agențiile de aplicare a legii și a mărit substanțial prerogativele organelor guvernamentale în ceea ce privește utilizarea mijloacelor tehnice de supraveghere a persoanelor pe parcursul investigațiilor cu privire la securitatea națională, anchete ce pot avea ca efect restrângerea temporară a exercițiului unor drepturi și libertăți cetățenești.

Printre măsurile luate de autoritățile americane, imediat după dezastrul din 11 septembrie 2001, se numără:

– extinderea competențelor serviciilor secrete de a culege informații și date „sensibile" de la furnizorii de servicii Internet;

– înființarea la puțin timp după atentate a Biroului de Influență Strategică („Office of Strategic Influence"-O.S.I.), în cadrul Pentagonului, pentru a sensibiliza pozitiv modul de percepere a politicii Washingtonului de către opinia publică[48];

[48] Oficiul a fost desființat la 26 februarie 2002 ca urmare a reacției mediatice negative față de legalitatea acțiunilor de transmitere a unor știri sau trimiteri de e-mailuri, favorabile americanilor, adresate presei sau unor înalți oficiali.

– crearea la 30 octombrie 2001 a Centrului de monitorizare a țintelor teroriste străine („Foreign Terrorist Asset Tracking Center") ce are ca obiect de activitate, printre altele, verificările efectuate, în contextul măsurilor restrictive de acordare de vize imigranților și reținerea acestora pe o perioada nedeterminată, de către Serviciul pentru Imigrări și Naturalizări, a celor suspectați de implicarea în acte teroriste;

– decembrie 2001, demararea „Operațiunii Scutul Americii" („Operation Shield America") de către Serviciul Vămilor (Custom Service) pentru a contracara posibilitatea teroriștilor de a achiziționa bunuri și tehnologii sensibile, produse în SUA;

– întărirea colaborării între FBI și CIA prin înființarea Biroului de Informații („Office of Intelligence" — O.I.);

– decembrie 2002, constituirea Departamentului Securității Interne (Department of Homeland Security – DHS) cu competențe în domeniile securității transporturilor și frontierelor, organizării reacției în situații de urgență, luării contramăsurilor în cazul unor atacuri chimice, biologice sau nucleare, precum și atribuții de protejare a structurilor de securitate[49].

Totodată ar fi util ca și la nivel european să se înființeze un organism specializat în domeniul antiterorist, după modelul american al Centrului Integrat pentru Amenințarea Teroristă (Terrorist Threat Integration Center — TTIC) înființat în luna ianuarie 2003 și devenit funcțional cinci luni mai târziu, la 1 mai 2003.

Centrul are competența de a analiza informațiile referitoare la amenințări teroriste obținute de la toate structurile cu atribuții în domeniul culegerii de informații și din afara SUA, este condus de un director, numit de șeful CIA, iar personalul este format din 180 000 de angajați din care 300 sunt agenți și experți în antiterorism, ce provin de la toate

[49] President Unveils new antiterrorist strategy „Jane's Terrorism & Security Monitor, sept.2002, p.15.

agențiile de spionaj (indiferent de departamentul cărora li se subordonează sau de mijloacele utilizate pentru obținerea informațiilor de interes strategic) și au acces la toate informațiile aflate la dispoziția guvernului, de la simple rapoarte de teren la evaluări analitice complexe[50].

Atributele speciale ale acestei structuri de securitate se referă la:

– întocmirea unei hărți zilnice („dailly threat matrix") în care sunt analizate și evaluate amenințările teroriste pentru uzul Președintelui și a altor factori de decizie din agențiile de informații sau cu competențe în domeniu, principalul beneficiar fiind Departamentul Securității Interne (Department of Homeland Security — D.H.S.);

– constituirea unei baze de date actualizată permanent, referitoare la teroriști și persoanele suspectate de a fi implicate în astfel de acte, accesibilă tuturor persoanelor cu atribuții în domeniul realizării siguranței.

Un alt demers american ce se impune a fi amintit este Centrul de Monitorizare a Terorismului (Terrorist Screening Center — TSC), înființat la 1 decembrie 2003, printr-o directivă prezidențială, exemplu ce ar putea fi urmat de asemenea și la nivel european. Centrul este de fapt o mega-agenție, controlată de Congres și administrată de FBI, care reunește bazele de date referitoare la teroriștii actuali și potențiali din cadrul Departamentul Justiției, Departamentul de Stat, Departamentul Securității Interne și a celorlalte structuri informative sau cu atribuții de securitate.

Această performantă bază de date este destinată concentrării informațiilor despre teroriști aflate în deținerea tuturor agențiilor de informații și de aplicare a legii și permite accesul federal al utilizatorilor abilitați. Inițiativele americane amintite sunt justificate ținând cont de eșecul înregistrat de structurile de securitate americane la 11 septembrie 2001.

[50] *USA centralises terror theaat assessments*, în „Jane's Intelligence Review", march, 2003, p. 4.

De altfel, așa cum sublinia prof. univ. dr. Cristian Troncotă[51]: „Istoria serviciilor secrete e plină de momente de tensiune și dramatism, de succese și de amare înfrângeri. Și unele și celelalte sunt trecute tot în contul oamenilor, care sau încumetat să poarte povara unor grele misiuni, cu conștiința că-și slujesc țara".

În prezent, SUA acordă prioritate măsurilor de protecție față de atacurile teroriste, informatice și de spionaj, precum și combaterii eficiente a infracțiunilor bazate pe violență sau înaltă tehnologie, corupției, spălării de bani sau altor forme de manifestare a crimei organizate, paralel cu dotarea modernă a agențiilor de aplicare a legii și întărirea cooperării la nivel internațional, federal, statal și local.

Țările europene, și în special cele care au trimis trupe în Irak, se confruntă acum cu teama că ar putea deveni următoarele ținte ale atentatelor teroriste puse la cale de militanți islamiști, sens în care își reevaluează politicile de securitate și vulnerabilitățile în domeniile ce pot afecta securitatea națională, prin efectele interdependente, difuze, multidirecționale bazate pe mobilitate, diversitate, coerență și complementaritate atât în spațiul intern cât și internațional.

Astfel, schimbările în politica de securitate națională presupun teorii noi dar și soluții pragmatice[52], încât proiectarea strategiilor de apărare să pună accent pe:

– un nou management al crizelor neconvenționale, nearmate;

– dezvoltarea sistemului integrat de gestionare a riscurilor și mai ales conectarea acestuia la organismele existente în NATO și UE;

– identificarea de noi soluții pentru consolidarea capacităților necesare de răspuns la crize, de combatere a tero-

[51] Cristian Troncotă, *Mihail Moruzov si frontul secret*, Editura Elion, București, 2004, p. 11.

[52] Ion Pleșu, *Managementul crizelor neconvenționale*, http:/www.presamil.ro/SMM/2003/09 pag% 2034–35.htm.

rismului și de asistență umanitară la nivel subregional și regional;

– stabilirea de noi parametri în controlul riscurilor și al vulnerabilităților tehnologice la obiectivele naționale de interes strategic;

– identificarea de noi modalități de îmbunătățire a avertizării naționale și internaționale pentru prevenirea evenimentelor transfrontaliere;

– operaționalizarea forțelor destinate să participe la prevenirea actelor teroriste, dar și a celor pentru intervenția postdezastru;

– armonizarea legislației și a procedurilor specifice cu reglementările internaționale și cu standardele U.E. privind forțele de ordine publică și serviciile de urgență;

– cunoașterea dimensiunii impactului psihologic și mediatic asupra populației apărut în urma atacurilor teroriste;

– gestionarea crizelor mediatice și de comunicare instituțională;

– redefinirea parteneriatului cu societatea civilă și întărirea controlului informațiilor ce vizează siguranța națională;

– asigurarea unui echilibru între dreptul la libera informare și necesitatea protejării informațiilor clasificate;

– realizarea unei intervenții specializate pentru controlul riscurilor și vulnerabilităților, a prognozării, alarmării, semnalizării unui eveniment a salvării, evacuării și acordării primului ajutor după comiterea acestuia, a reabilitării zonelor afectate și ajutorării sinistraților.

Un pas extrem de important în lupta împotriva terorismului e reprezentat de hotărârea guvernelor de a trata amenințările fenomenului terorist și de a consacra inițiativele instituțiilor internaționale pe plan legislativ.

Printre elementele reacției la nivel global pot fi amintite:

– eforturile pentru prevenirea și eliminarea acțiunilor teroriste, atacurile cu bombe, terorismul aerian și luările de ostatici;

– combaterea acțiunilor teroriste din domeniul financiar pentru procurarea și diseminarea armelor de distrugere în masă;

– urmărirea, prinderea, extrădarea sau judecarea teroriștilor și detenția lor în siguranță și cu respectarea reglementarilor adoptate la nivel internațional;

– implementarea Rezoluției nr. 1373 a ONU adoptată la 28 septembrie 2001 și adaptarea legislației interne din fiecare țară la standardele internaționale privind lupta împotriva terorismului;

– implementarea Convenției ONU împotriva terorismului;

– adoptarea Convenției Internaționale cu privire la combaterea actelor de terorism nuclear;

– descoperirea și eliminarea surselor de finanțare a mijloacelor de comunicații ale structurilor de organizare teroristă (firme, ONG-uri etc.);

– adoptarea unor măsuri de control al circulației persoanelor și reducerea fenomenelor de emigrație ilegală;

– susținerea Organizației Internaționale a Aviației Civile pentru implementarea unor măsuri sporite de asigurare a securității zborurilor și a securității pe aeroporturi.

Comunitatea euro-atlantică lărgită consolidată și cât mai bine integrată în privința cooperării în lupta împotriva terorismului reprezintă nucleul acțiunii globale împotriva flagelului, ce a devenit *„inamicul public nr. 1"* al stării de siguranță al statelor lumii.

POLITICI DE SECURITATE

Ultimele evoluții din domeniul relațiilor transatlantice și al raporturilor dintre principalele organizații responsabile pentru securitatea europeană — NATO și Uniunea Europeană — semnalizează o perioadă de mari transformări și

renegocieri ale principalelor aranjamente de securitate pentru spațiul euro-atlantic.

Lărgirea NATO înseamnă și intrarea „de facto", cu drepturi și îndatoriri în marea coaliție a forțelor combatante pe frontul contra terorismului mondial, în general a amenințărilor transfrontaliere. Numai că noii aliați vor contribui la activitatea Alianței atât cu punctele lor forte cât și cu propriile vulnerabilități ce pot atrage atenția teroriștilor.

Necesitatea redefinirii parteneriatului dintre America și Europa în contextul generat de intervenția în Irak și demersurile europenilor (mai ales după atentatul de la Madrid din 11 martie 2004) de edificare a dimensiunilor comune de apărare a devenit subiectul principal pe agenda experților în domeniul securității internaționale.

În general politica de securitate are o accepțiune publică ce poate fi vizualizată „ca o rețea de decizii legate între ele prin alegerea obiectivelor, a mijloacelor și resurselor alocate pentru atingerea lor în situații specifice"[53].

Securitatea se bazează atât pe stabilitatea politică cât și pe cea militară, acestea fiind într-o relație de condiționare complementară. Un sistem mobil de securitate europeană va putea fi edificat numai dacă vor fi consolidate cele două componente. Politica de securitate bazată pe cooperare[54] presupune renunțarea la orice idee de a impune stabilitatea prin mijloace de confruntare. Scopul este promovarea cooperării în vederea prevenirii conflictelor în sfera politică și a reducerii pericolului confruntării armate. De asemenea aceasta urmărește evitarea escaladării potențialelor conflicte, punând un accent deosebit pe promovarea deschiderii și a transparenței. Apărarea și securitatea colectivă, pe de o parte și securitatea bazată pe cooperare pe de altă parte

[53] Marian Zulean, *Armata și Societatea în tranziție*, Editura Tritonic, Bucuresti, 2003, p. 121.

[54] Petre Anghel, *Instituții europene și tehnici de negociere în procesul integrării*, http:/www.unibuc.ro/eBooks/stiințe Pol /anghel/8.html.

sunt instrumente fundamental diferite, dar complementare ale politicii internaționale de securitate.

Accentul din cadrul acestui concept este pus nu doar pe recunoașterea problemelor ce interacționează cu un conflict militar ci și pe luarea în considerație a evenimentelor ce pun în pericol statul național și cetățenii acestuia, odată cu ariile transnaționale sau regionale de impact, ca urmare a diversității amenințărilor asimetrice la adresa securității statului.

Totodată printre efectele pozitive ale securității prin cooperare se numără: deschiderea accesului la comerțul internațional, reducerea costurilor pentru securitate (având în vedere presiunile de restrângere a cheltuielilor) paralel cu împiedicarea statelor de a acumula mijloace de acțiune ofensivă împotriva altor state.

Modelul *„cooperare pentru securitate"* (*cooperative security model*) a fost analizat de Richard Cohen[55] în revista Centrului European de Studii de Securitate *„George Marshall"* și urmărește să pună în valoare printre altele eficacitatea NATO care are capacitatea de a asigura securitatea și în afara teritoriului statelor ce o compun.

Sistemul strategic al cooperării pentru securitate concentrează în jurul unui nucleu mai multe state democratice, între care există strânse legături concretizate în alianțe sau instituții cu caracter formal sau informal care acționează în baza unor principii comune și cooperează în domeniile: economic, politic și al apărării.

O extensie a conceptului de securitate, aceea de „securitate colectivă", promovată inițial de către Liga Națiunilor, a fost preluată și continuată prin organizații precum Organizația Națiunilor Unite (prin art.41 și art.42) sau Con-

---

[55] Cohen Richard, *From Individual Security to International Stability in Cooperative Security: New Horizons for International Order*; Cohen, Richard și Mihalka, Lichael, în „The Marshall Center Papers", nr. 3 aprilie 2001, citat de Aurel Băloi, *Analiza securității internaționale: delimitarea conceptuală*, http:/www.studiu de securitate.ro/indicatori_securitate.html.

ferința pentru Securitate și Cooperare în Europa (C.S.C.E. devenită ulterior O.S.C.E.). Acest concept presupune că un grup de state suverane își promit reciproc să se protejeze împotriva unui atac declanșat de o națiune, ce este parte a acelei organizații.

O altă accepțiune a conceptului de securitate — „apărarea colectivă" constă în aceea că un grup de state se organizează pentru a se proteja împotriva unei agresiuni externe (ex. Tratatul de la Varșovia, Organizația Atlanticului de Nord — NATO care în prezent promovează „securitatea prin cooperare").

Relevant în sistemul de cooperare pentru securitate sunt atât ideea de bază a diversității de roluri și a diviziunii sarcinilor cât și obiectivele de securitate națională ale fiecărui stat ce interacționează, contribuind la coerența și adaptarea întregului sistem prin *„patru inele de securitate"* („the four rings") axate pe:

– securitatea individuală (care vizează promovarea și protejarea drepturilor omului în cadrul teritoriului național);

– securitatea colectivă (se referă la menținerea păcii și stabilității în spațiul comun al statelor semnatare);

– apărarea colectivă (presupune protecția reciprocă împotriva unei agresiuni externe);

– promovarea stabilității (se referă la inducerea activă a stabilității în alte spații unde conflictele amenință securitatea realizată în cel de-al treilea inel, folosindu-se mijloace politice, economice și dacă este necesar, militare.

În esență, securitatea prin cooperare vizează activitatea interactivă dintre state și organizații internaționale care contribuie la eliminarea războiului (fără a fi neapărat îndreptat împotriva unui anumit stat sau grup de state) sau a consecințelor acestuia, strategie care reclamă eforturi conjugate ale statelor, organizațiilor, *„actorilor"* nestatali de a obține securitatea lor ca răspuns la amenințările sau provocările comune. Una din premisele acestei strategii de cooperare constă în faptul că securitatea este indivizibilă ca rezultat al efortului comun.

Aplicarea sistemului „securității prin cooperare" conturează însă atât dificultatea de angajare a tuturor armatelor într-un astfel de sistem (în special a celor cu potențial ridicat) cât și disfuncționalitățile de depășire a decalajelor ce privesc securitatea și insecuritatea, dintre emisfera nordică și cea sudică a globului, la care se adaugă problema menținerii statelor națiune ca unități viabile ale puterii[56].

Cu privire la securitatea colectivă, relevant este că aceasta vizează o obligație politică reciprocă a statelor membre ale unui act juridic internațional (tratat, convenție etc.) de a apăra integritatea celorlalte părți semnatare.

Securitatea colectivă are ca scop realizarea securității în cadrul unui grup de state suverane. Diferența dintre securitatea colectivă și securitatea comună rezidă în opozabilitatea obligațiilor. În cazul celei din urmă, obligațiile unui stat vizează ansamblul statelor în timp ce în cazul securității colective eforturile de responsabilitate sunt direcționate spre părțile semnatare ale unui instrument juridic internațional.

Securitatea individuală se suprapune noțiunii de securitate națională, iar apărarea colectivă concentrează angajamentul tuturor statelor de a se apăra reciproc de o agresiune exterioară.

Astăzi se încearcă o relansare a conceptului de „securitate prin cooperare", o redefinire a unui sistem de securitate, în care toate națiunile și toate organizațiile de securitate — fie ele sub-regionale, regionale, internaționale sau globale — trebuie să-și coordoneze eforturile și să coopereze mai strâns pentru atingerea acelorași obiective comune, „pacea globală" find înțeleasă nu doar ca lipsă a războiului, ci și ca un mediu de dezvoltare economică și socială[57].

Există organizații — Uniunea Europeană, NATO, Organizația Tratatului din Sud — Estul Asiei (SEATO) — care

[56] Stanford News, Stanford Center for International Security and Arms Control Conference.

[57] M. Zulean, *op.cit.*, p. 87.

au la bază un tratat în care este stipulată apărarea reciprocă în cazul în care un stat membru este amenințat sau este deja subiect al unui atac militar din partea unui stat sau a unui grup de state din afara tratatului.

Semnificativ în acest sens este obiectivul esențial și permanent al NATO[58] așa cum a fost enunțat în tratatul de la Washington și care constă în apărarea libertății și securității tuturor membrilor săi prin mijloace politice și militare. Securitatea în cadrul Alianței furnizează una dintre bazele indispensabile unui cadru de stabilitate regională euro-atlantică, fondat pe dezvoltarea de instituții democratice și pe angajamentul de a reglementa neînțelegerile în mod pașnic astfel încât nici o țară să nu fie în măsură să recurgă la intimidare sau la constrângere împotriva unei alte țări prin amenințarea cu forța sau prin folosirea ei.

Modul cum funcționează garanțiile de securitate a fost prevăzut în celebrul art. V care precizează că în cazul unui atac asupra unuia dintre membrii NATO, acesta ar fi considerat ca îndreptat împotriva tuturor membrilor Alianței și toate părțile contractante vor lua *„măsurile pe care le cred necesare inclusiv folosirea forței armate pentru a stabili securitatea NATO"*. Totodată în art. 4 al Tratatului părțile semnatare și-au asumat obligația de a se consulta reciproc atunci când *„integritatea teritorială, independența politică sau securitatea unui dintre state este amenințată"*.

Atacurile teroriste din 11 septembrie 2001, soldate cu mii de morți, îndreptate asupra simbolurilor puterilor economice

[58] Alianța a fost constituită la 4 aprilie 1949 în plină blocadă a Berlinului, iar documentul de înființare, tratatul, a fost semnat la Washington grație eforturilor conjugate ale președintelui Truman, membru al Partidului Democrat și senatorului republican Vandenberg, președintele Comisiei pentru Relații Externe. Statele fondatoare ale NATO au fost SUA, Canada și cele semnatare ale tratatului de apărare colectivă de la Bruxelles din 1948 (modificat în 1954 care avea să pună bazele a ceea ce se va numi mai târziu Uniunea Europei Occidentale) respectiv Marea Britanie, Franța și țările din Beneleux, la care s-au alăturat Danemarca, Islanda, Italia, Norvegia și Portugalia.

financiare și militare ale SUA, au oferit un inedit prilej de reacție nu numai statelor semnatare ale Alianței (care și-a pus problema incidenței art. V din Tratat) dar și comunității internaționale obligată să fie martora oculară *„în direct"*, prin intermediul televiziunii, la acest eveniment unic prin modul de declanșare a agresiunii.

Atacurile teroriste nu au reușit să submineze puterea politică, economică, financiară și militară ale SUA și nici capacitatea sa de a o proiecta global. Dimpotrivă, atât aliații tradiționali ai SAU cât și numeroase alte state motivate de repulsia provocată de atrocitățile comise și-au manifestat opțiunea pentru un sprijin fără echivoc, în lupta împotriva unei amenințări comune — terorismul internațional.

Asumat la Praga *„Planul de acțiune al Parteneriatului Euroatlantic împotriva terorismului"* a stabilit coordonatele cooperării interaliate, activând resorturile reacției unitare împotriva terorismului.

Într-un context internațional adesea schimbător, NATO deține în prezent un rol politic esențial în întărirea securității euro-atlantice, îndeosebi după adoptarea la summitul de la Washington din 1999, a unui nou concept strategic al Alianței, semnificative fiind și documentele adoptate după evenimentele teroriste din 11 septembrie 2001, precum:

– Declarația Adunării Consiliului Nord-Altantic (11 septembrie 2001);

– Declarația Adunării Consiliului Nord-Altantic (12 septembrie 2001);

– Declarația privind lupta împotriva terorismului, Adunarea Parlamentului NATO (23 octombrie 2001).

La rândul său Uniunea Europeană a adoptat decizii importante și a dat un nou impuls eforturilor sale de întărire a securității și dimensiunii de apărare. Dezvoltarea unei politici externe și de securitate comună, include și definirea progresivă a politicii de apărare preconizată de Tratatul de la Amsterdam, compatibilă cu politica de securitate și de apărare instituită prin Tratatul de la Washington. Totodată Uniunea Europeană este preocupată de finalizarea propriilor

reforme instituționale interne, precum și de eficiența dezbaterilor declanșate pe tema viitorului Europei, a construcției politice pe continent.

În acest context devine tot mai evident faptul că interesele și obiectivele de securitate ale statelor pot fi realizate doar prin cooperare internațională care să se manifeste nu numai în situații limită ci și în tot contextul problematic — economic, social, financiar ale lumii de azi.

Această nouă resolidarizare a statelor lumii se poate exprima în toate aceste domenii prin stabilirea unor forme de acțiune conjugată a tuturor națiunilor care împărtășesc interese și valori comune.

ROMÂNIA ÎN NOUL CONTEXT EUROPEAN, COORDONATE ALE SECURITĂȚII NAȚIONALE

Aurel Dumitru

Tendințele de evoluție a mediului de securitate la nivel regional sunt prefigurate în egală măsură de condițiile actuale și de tendințele globale, având sorgintea în situația foarte complexă și contradictorie ce caracterizează majoritatea zonelor lumii, în special Europa.

Din perspectiva enunțată, mediul de securitate european se caracterizează prin:

– existența concomitentă a statelor puternic structurate și a celor în curs de reorganizare, formare sau reformare;

– coexistența situațiilor de pace cu cele de conflict sau potențial conflict, având determinări de natură diferită, concomitent cu internaționalizarea unora dintre acestea;

– existența unui echilibru (destul de fragil) între riscuri, amenințări și pericole pe de o parte și starea de securitate, cel puțin în plan zonal, pe de altă parte;

– intensificarea eforturilor unor state aflate în curs de restructurare pentru îndeplinirea cerințelor de integrare în structurile europene și euro-atlantice de securitate;

– existența intereselor divergente ale unor state sau grupuri de state, precum și ale unor grupuri din interiorul unor state cu dorințe autonomiste, interese care converg către stări de tensiune de natură etnică sau religioasă, ce pot degenera în stări de conflict ori dispute de altă natură;

– persistența unor divergențe de natură frontalieră;

– evoluții economice și sociale asimetrice, cu implicații majore în plan geopolitic și geostrategic;

– pătrunderea și extinderea fundamentalismului islamic, în unele cazuri excelând prin radicalitate;

– adâncirea decalajelor economice, sociale și tehnologice dintre diferite țări și zone ale continentului;

– sporirea efectelor și a influienței amenințărilor de natură nemilitară asupra evoluțiilor regionale din domeniul securității și nu numai;

– important de subliniat — rolul pe care l-au jucat și probabil îl vor juca în continuare Statele Unite ale Americii pentru securitatea Europei, aspect care trebuie luat în considerare ori de câte ori se evaluează sau se proiectează problemele securității pe continentul european, simultan cu mutațiile ce au avut loc de-a lungul ultimei jumătăți a secolului XX.

Referitor la tendințele de evoluție a securității continentului european, unul dintre cele mai semnificative elemente este relația NATO-UE, de multe ori însoțită de întrebări de genul: „Care vor fi orientările pe care le-ar putea urma cele două structuri ale securității regionale: independent sau împreună?"; „Care ar putea fi implicațiile și urmările evoluțiilor viitoare?" Așa cum am subliniat, Europa ar putea reprezenta unul dintre cele patru triunghiuri strategice care se conturează la nivel global, acesta bazându-se la rândul lui pe trei piloni: Uniunea Europeană, SUA, Rusia. În această variantă se pune firesc întrebarea: ce se va întâmpla cu NATO?

În studiile unor specialiști americani, se vorbește despre evoluția foarte strânsă a relației Inițiativa Europeană de Apărare și Securitate — Uniunea Europeană, ceea ce duce inevitabil la ideea coexistenței UE cu o Alianță Nord-Atlantică, având însă o importanță redusă, limitată, într-o variantă, la aplicarea art. 5 al Tratatului — o parte din responsabilitățile acesteia, inclusiv operațiile de sprijin al păcii, putând fi preluate de către UE, ori la schimbarea dramatică a NATO, mergând, în varianta pesimistă, până la dispariția organizației.

Studiile unor analiști europeni referitoare la perspectivele Uniunii Europene ca actor internațional de securitate relevă o „evoluție paralelă" a NATO și UE, cu specialzarea diferențiată a celor două organisme de securitate, primei revenindu-i responsabilități preponderent militare, de rezolvare a

conflictelor armate, iar celei de a doua, responsabilități preponderent civile, de rezolvare a crizelor prin operații de sprijin a păcii și umanitare. Seminficativ în acest sens este studiul Grupului de la Venusberg, intitulat „Dezvoltând Uniunea Europeană ca actor internațional de securitate" — o strategie de acțiune, din care decurg următoarele aspecte esențiale:

– UE trebuie să adopte un nou concept strategic, care să ducă la refacerea credibilității în plan diplomatic și la integrarea Europei pe baza a trei criterii — legitimitate politică, posibilități militare și capabilitatea de a-și asuma noile responsabilități;

– întărirea organismelor proprii existente și crearea altora noi, corespunzătoare cerințelor rezultate din actualele responsabilități;

– până în anul 2015, UE trebuie să fie în măsură să desfășoare operații de tip KOSOVO pe baza propriilor capacități civile și militare de planificare a apărării, de gestionare conceptuală și doctrinară a crizelor;

– autonomia operațională se va putea realiza prin crearea unor instituții și structuri similare celor ale NATO, în special în domeniul informațiilor strategice, comunicațiilor permanente, de supraveghere și cercetare tactică, precum și de transport și logistice, la nivel strategic și tactic;

– trecerea, începând cu anul 2003, la asumarea graduală a misiunilor forțelor și la creșterea responsabilităților în concordanță cu evoluțiile precizate în Tratatul de la Amsterdam.

În ceea ce privește Organizația Tratatului Nord Atlantic, studiile prefigurează mai multe variante de evoluție, mergând până la alternativele cele mai pesimiste. În acest sens, unii analiști americani întrevăd trei variante distincte de evoluție:

– în cazul unei Europe integrate ca uniune economică și monetară, NATO ar putea juca încă un rol foarte puternic și va acoperi o gamă foarte largă de misiuni, de la cele de

sprijin al păcii și umanitare, la cele bazate pe articolul 5 al Tratatului;

– într-o Europă confederativă, în care Germania, Franța și Marea Britanie vor juca un rol tot mai important, NATO ar putea evolua spre diminuarea propriilor responsabilități, limitându-și implicarea la apărarea colectivă, în virtutea articolului 5 al Tratatului;

– cea de a treia variantă arată o Europă federală, cu diminuarea dramatică sau chiar dispariția Alianței Nord-Atlantice și preluarea de către Uniunea Europeană a tuturor problemelor de securitate.

Cel de al doilea pilon de securitate al triunghiului de securitate, SUA, ar fi caracterizat potrivit părerilor unor specialiști americani, de următoarele perspective de evoluție:

– SUA va rămâne o forță în plan politic, militar și cultural până spre anii 2025, cu rol semnificativ în mediul internațional;

– știința și tehnologia vor continua să progreseze și vor deveni tot mai mult disponibile și utilizabile în toată lumea, însă beneficiile acestora vor fi tot mai neuniform distribuite;

– chiar dacă lumea va cunoaște o creștere economică, disproporțiile beneficiilor vor spori, iar diferențele de proprietate vor persista sau se vor amplifica;

– aspectele internaționale ale afacerilor și comerțului vor continua să se extindă, ducând la crearea unei infrastructuri globale, ușor de afectat, deci mult mai vulnerabilă;

– organizațiile neguvernamentale (pentru refugiați, grupurile de apărare religioasă și etincă, cele care luptă pentru protecția mediului sau pentru rezolvarea altor probleme, asociațiile internaționale profesionale etc.) vor continua să crească în importanță și număr, ceea ce va afecta inclusiv interesele SUA;

– vor apărea importante probleme referitoare la suveranitate, iar SUA vor avea interes să colaboreze în interiorul unor organizații internaționale — actori nestatali;

– SUA va rămâne principala putere militară în lume, ceea ce îi va aduce atât responsabilități sporite cât și probleme noi de rezolvat;

– armele de distrugere în masă și războiul informațional vor prolifera spre o largă varietate de actori statali și nestatali, iar menținerea unei superiorități în aceste domenii va fi esențială, ca de altfel și investițiile pentru găsirea unor noi forme de apărare împotriva acestora.

Cel de-al treilea pilon de securitate al triunghiului european, Federația Rusă, cu părțile ei pozitive ori negative și cu valorile sau cu greutățile sale, aduce în atenție următoarele variante probabile de evoluție:

– o Rusie autoritară care va avea un comportament activ față de vecini, față de Europa, NATO și Orientul Apropiat, cu o economie necompetitivă și neatractivă, continuând vânzările de armament, cu forțe de securitate capabile să mențină actualele structuri federale și țara „unită" gata oricând să amenințe cu folosirea armelor nucleare;

– o Rusie confuză, care va deveni un partener dificil de dialog — în special cu privire la extinderea în continuare a NATO — cu un potențial militar totuși suficient pentru a exercita controlul la nivel regional, în primul rând nuclear;

– o Rusie democratică, oreintată spre economia de piață, partener cooperant al NATO și UE, cu interese regionale în exindere, dar favorabilă procesului de globalizare.

Având în vedere elementul de noutate din relațiile NATO-Rusia cât și importanța deosebită a acestei relații în configurarea noilor raporturi de securitate de pe continentul european, în cele ce urmează, voi încerca să schițez principalele trăsături ale acestei relații.

De la crearea Alianței Nord-Atlantice, în 1949, rolul său a evoluat în mod considerabil, mai ales după încheierea Războiului Rece, când s-a schimbat radical situația militară și politică din Europa. Reducerea pericolului amenințării unei confruntări militare directe a deschis ample posibilități în abordarea problemei securității europene într-o manieră novatoare și pozitivă.

În noul context strategic, Alianța a reușit o definire mai largă a securității și a lansat o vastă strategie de parteneriat și cooperare în întregul spațiu euro-atlantic. NATO a urmat un proces continuu de adaptare internă și externă, care i-a permis o funcționare mai eficientă și flexibilă în vederea abordării noilor provocări legate de conflicte naționale, violență etnică, catastrofe naturale și, mai ales, de terorismul internațional.

Sfârșitul Războiului Rece a determinat restructurări profunde ale Alianței, din punct de vedere politic și militar, care au condus la crearea unor noi structuri de cooperare în domeniul securității, împreună cu țări care nu sunt membre NATO și cu alte organizații internaționale, cu rol în îndeplinirea unor misiuni de menținere a păcii și de gestionare a crizelor.

Alianța a stabilit cadrul de colaborare strânsă cu țări care nu sunt membre NATO prin înființarea unor organisme, cum ar fi: Consiliul Parteneriatului Euro-Atlantic (CPEA), Inițiativa Parteneriatului penru Pace (PPP), Consiliul Comun Permanet NATO-Rusia, Comisia NATO-Ucraina și Dialogul Mediteranian. Toate aceste organisme au permis dezvoltarea unor relații bilaterale și multilaterale între NATO și celelalte țări nemembre, care să satisfacă nevoile de securitate ale partenerilor, contribuind astfel la securitatea zonei euro-atlantice în ansamblul ei.

Încă din anul 1990, NATO a promovat, în zona euro-atlantică, *parteneriatul și cooperarea cu țările din Europa centrală și de Est și cu fostele republici sovietice.* O atenție deosebită a fost acordată dezvoltării cooperării cu Rusia, partener indispensabil în realizarea sistemului european global de securitate.

Membru fondator al Consiliului de Cooperare Nord-Atlantic, încă din 1991, Rusia a aderat la Parteneriatul pentru Pace în anul 1994. Preocupările NATO pentru dezvoltarea unor relații de cooperare cu Rusia, radical diferite de cele avute până atunci, au devenit mai evidente în anul 1996, acestea materializându-se, ulterior, prin semnarea, la Paris,

la 27 mai 1997 a *Actului fondator referitor la relațiile, cooperarea și securitatea mutuală între NATO și Federația Rusă.* Acest document a oferit o bază nouă și reală pentru un parteneriat puternic și durabil între cele două părți, în scopul de a construi împreună o pace durabilă și deschisă tuturor, în regiunea euro-atlantică. Semnarea Actului fondator a fost urmată de crearea Consiliului Comun Permanent NATO-Rusia, un organism de cooperare în cadrul căruia NATO și Rusia s-au consultat periodic asupra unor probleme politice și de securitate privind menținerea păcii, securitatea nucleară, conversia industriei de apărare, controlul armamentului și protecția mediului înconjurător.

Evenimetele tragice din 11 septembrie 2001 au pus în evidență necesitatea ca NATO să desfășoare o acțiune globală și concordantă pentru a răspunde amenințărilor globale, legate de terorismul internațional. Astfel, cu prilejul reuniunii extraordinare desfășurate la 12 septembrie 2001, Consiliul Comun Permanent NATO-Rusia a exprimat voința comună a membrilor săi de a lupta împreună contra terorismului. Ulterior, la 23 octombrie 2001, președintele rus, Vladimir Putin și secretarul general NATO, lordul George Robertson, s-au întâlnit la Bruxelles pentru a examina posibilitățile intensificării cooperării dintre Rusia și NATO.

Pentru prima dată în istoria postbelică s-a creat o conjunctură în care interesele naționale pe termen lung ale Rusiei și SUA coincid.

Unul dintre cei mai importanți analiști militari ruși, Vitali Țâghicico, afirma într-un articol publicat la 21 mai a.c. că *„doar o alianță cu America ar putea face din Rusia unul dintre cei mai influienți jucători pe scena mondială și doar o cooperare ruso-americană ar putea duce la soluționarea numeroaselor probleme economice cu care se confruntă statul rus".*

După atentatele din SUA, Actul de bază semnat în 1997, precum și Consiliul Comun permanent Rusia-NATO (CCP) nu mai corespundeau noilor relații internaționale. Declarația comună a președinților George Bush – Vladimir Putin de

la Crowford, Texas, nota că *„...Rusia și Statele Unite vor conlucra alături de NATO și alte state NATO cu scopul de a ameliora, întări și intensifica relația dintre Alianță și Rusia, în vederea dezvoltării unui mecanism nou și efectiv de consultații, cooperare, adoptare de decizii comune și realizare de acțiuni coordonate comune"*.

La întâlnirea de la Bruxelles, din 7 decembrie 2001, organizată la nivelul Consiliului Comun Permanent NATO-Rusia s-a lansat inițiativa creării unui nou consiliu și a unui nou parteneriat care să definească și să caute noi căi de exploatare a posibilităților de acțiune comună.

Consiliul Nord-Atlantic, reunit la Reykjavik, la 14 mai 2002 a pus în discuție formula în care se va concretiza noua relație între NATO și Rusia. Cu acest prilej a fost aprobată semnarea unei *Declarații comune*, elaborată pe baza principiilor menționate în Actul fondator, care să stabilească mecanismele de consultare în vederea obținerii unui consens asupra unor probleme de imporatnță majoră pentru dezvltarea cooperării, luarea unor decizii în comun și desfășurarea unor acțiuni comune.

În scopul semnării acestei Declarații comune și pentru a marca împlinirea a 5 ani de când Rusia și țările membre NATO au semnat *Actul fondator* referitor la relațiile, cooperarea și securitatea mutuală dintre NATO și Federația Rusă, la 28 mai 2002, a fost organizat summit-ul de la Roma, la nivel de șefi de stat și de guvern din statele membre NATO și Federația Rusă.

Declarația intitulată *„Relațiile NATO-Rusia — o calitate nouă"* afirmă că, la începutul secolului XXI-lea, trăim într-o lume nouă, caracterizată de interdependențe, de amenințări și provocări noi, fără precedent, care impun răspunsuri unitare adecvate. În aces context, NATO și Federația Rusă au decis să deschidă un capitol nou al relațiilor lor, în domenii de interes comun. Pe baza Actului fondator și a inițiativei lansate pe 7 decembrie 2001 s-a decis crearea Consiliului NATO-Rusia.

Consiliul — care înlocuiește Consiliul Comun Permanent va constitui un mecanism de consultare, de stabilire a consensului, de cooperare, decizie și acțiune comună pentru toată gama de probleme referitoare la securitatea euro-atlantică. Consiliul va reprezenta cadrul și structura de îmbunătățire a relațiilor dintre NATO și Rusia, va aplica principiul consensului și va funcționa pe baza unui dialog politic constant pe problemele securității.

SECURITATEA ÎN SUD-ESTUL EUROPEI

Europa de Sud-Est reprezintă un complex de securitate individualizat, atât din punct de vedere geografic cât și din punct de vedere al civilizațiilor (zona este preponderent ortodoxă, dar și de interferență între spațiile catolic și islamic).

Din punct de vedere statal, spațiul este extrem de fragmentat și cuprinde: Albania, Grecia (este membru NATO și UE), FYROM (Fosta Republică Iugoslavă a Macedoniei), Turcia (este membru NATO), Cipru (plasat sub control ONU și divizat în regiuni administrative distincte - greacă și turcă), Bulgaria, Bosnia-Herțegovina, Iugoslavia (în cadrul său), Macedonia, Kosovo și Voievodina dețin prerogative proprii de autoadministrare), Croația, Slovenia, România.

Toate statele balcanice sunt membre OSCE și sunt incluse în Pactul de Stabilitate din Balcani. La Inițiativa Central-Europeană au aderat: România, Bulgaria, Macedonia, Slovenia, Albania.

Toate aceste țări sunt de asemenea incluse în procesul de extindere UE și NATO. În regiune acționează SECI (Inițiativa de Cooperare Sud-Est Europeană) și SEDM (Conferința miniștrilor apărării din Europa de Sud-Est).

În Bosnia-Herțegovina și Kosovo s-au desfășurat forțe de poliție și militare ONU și NATO de menținere a păcii.

Acest spațiu etalează o puternică prezență militară NATO și nord-americană, datorită importanței sale strategice de excepție.

Complexul de securitate din Europa de sud-est traversează un profund proces de restructurare politică, economică și militară.

SUA și NATO (în cadrul ONU și OSCE) controlează evoluțiile locale, orientate către: prevenirea, stoparea și gestionarea conflictelor armate și politice; democratizare; dezvoltarea economiilor de piață; integrarea în structuri regionale, europene și euro-atlantice de securitate.

ASPECTE ECONOMICE ALE SECURITĂȚII

Există o serie de slăbiciuni din acest punct de vedere în zonă, ce decurg din:

– sărăcia relativă a solului și subsolului;

– existența unei industrii grele depășită din punct de vedere tehnologic;

– slaba dezvoltare a infrastructurii;

– lipsa capitalului necesar investițiilor de modernizare industrială și de promovare a serviciilor;

– o piață puțin atractivă pentru marii investitori străini;

– persistența unor mentalități „neocomuniste" în zone din Albania, Iugoslavia;

– economia subterană ocupă un loc important în dinamica economică a regiunii;

– impactul negativ al războaielor și conflictelor armate locale (Iugoslavia, Bosnia-Herțegovina, Kosovo, Macedonia) asupra economiilor naționale și a circuitelor economice regionale;

– rezultate nefavorabile obținute în aplicarea reformelor de modernizare în fostele state socialiste;

– creșterea demografică vertiginoasă din anumite zone (Albania, Kosovo), în condițiile neimplementării reformelor economice, stagnării sau chiar regresului industriei;

– consecințele proceselor de regionalizare și mondializare economică.

Toate aceste probleme reprezintă un handicap în competiția pentru aderarea la NATO și UE și împiedică constituirea unei baze economice solide, care este indispensabilă cooperării economice în plan regional.

ASPECTE POLITICE ALE SECURITĂȚII

Dintr-o analiză profundă rezultă următoarele caracteristici:

– principala carență o constituie incapacitatea statelor-națiuni sau federații din zonă de a preveni și gestiona crizele locale;

– nu s-a încheiat procesul de remodelare politico-teritorială a regiunii, început după 1989. Există încă conflicte latente în Iugoslavia (între Muntenegru și Serbia), în Serbia (tendința de independență și autonomie în Kosovo și Voievodina) și în Macedonia;

– există încă proiecte de creare a unor state mari (Albania Mare, Serbia Mare, Bulgaria Mare), iar acest lucru a transformat zona în principalul „generator de insecuritate" din Europa;

– nu au fost asimilate pe deplin sistemele moderne de valori democratice (regimurile democratice s-au dezvoltat confuz și anemic);

– există încă reflexe autoritare ale liderilor și societății;

– există încă intoleranță politică.

Toate aceste elemente constituie obstacole reale în calea procesului de integrare europeană și euro-atlantică și este nevoie de asistență din partea organismelor internaționale.

ASPECTE CULTURALE ALE SECURITĂȚII

Problemele legate de cultură, tradiții au fost „sensibile" dintotdeauna în Europa și în special în Balcani deoarece:

– Europa de sud-est reprezintă un mozaic de popoare, culturi și religii;

– intoleranța este mai puternică decât toleranța constructivă și cooperarea;

– conflictele balcanice interetnice și interconfesionale s-au soluționat prin recurgerea la arme și purificare etnică (Croația, Serbia, Bosnia-Herțegovina, Kosovo);

– în 2001 în Iugoslavia și Macedonia s-a ajuns la o reglementare democratică, în concordanță cu valorile europene (respectarea identității etno-culturale și cooperarea politico-administrativă). În același spirit s-au relansat inițiativele de lărgire a autonomiei locale în Voievodina și punerea pe picior de egalitate a Serbiei cu Muntenegru;

– scopul comunității internaționale este de a crea un Kosovo multi-etnic, unde toate comunitățile, inclusiv cea sârbă să fie în siguranță și să participe la democratizarea societății;

– progresele în sfera drepturilor minorităților sunt destul de timide.

Toată această situație impune:

– inițiative;

– folosirea de instrumente economice, politice și militare;

– activitate intensă de educare în spiritul respectării drepturilor și libertăților civice, toleranței politice și religioase, cooperării și conviețuirii comune;

– nerezolvarea tensiunilor din acest spațiu se va solda cu amplificarea poziției zonei ca spațiu de insecuritate. Situația în zonă este gestionată de actori externi;

– caracteristicile securității la cele trei niveluri pot transforma toate aceste vulnerabilități în amenințări. Pe de altă parte, un conflict armat în orientul Mijlociu ar determina o scădere drastică a economiei în Balcani (zona este dependentă de petrolul arab și rusesc);

– încetarea asistenței economice internaționale și eșecul implementării monedei euro s-ar resimți negativ. Excluderea acestor state din procesul de integrare euro-atlantică reprezintă o amenințare la adresa securității;

– stabilitate în regiune poate fi grav afectată de expansiunea terorismului sau a fundamentalismului islamic sau ortodox;

– trebuie identificată o formulă politică de rezolvare durabilă și democratică a „problemei succesiunii iugoslave", iar acest lucru constituie un examen pentru toate instituțiile internaționale implicate în zonă (ONU, UE, NATO, OSCE);

– dinamica evenimentelor din această zonă a dovedit că securitatea depășește sfera de responsabilitate a unei singure țări;

– atât actorii regionali cât și cei internaționali consideră că cel mai mare obstacol către stabilitate și prosperitate al zonei este lipsa de instituții ale statului responsabile și eficace. Construirea de instituții este deci un element cheie prioritar. Fără această reformă, nici integrarea în structurile regionale nici în cele europene nu va avea rezultate. Fără un cadru instituțional puternic pentru exercitarea puterii, alegerile libere nu vor duce la guverne reprezentative și responsabile. Fără instituții puternice care să implementeze statul de drept există o mică probabilitate că statele vor putea oferi o protecție efectivă a drepturilor omului și ale minorităților, indiferent la ce convenții internaționale vor adera;

– fără structuri economice stabile, care să stabilească un climat favorabil pentru afaceri, nici privatizarea și nici liberalizarea comerțului nu va genera o creștere economică susținută;

– problema este că această construire de instituții este cel mai nedezvoltat segment al ajutorului internațional, care este centrat pe reconstrucție și ajutor umanitar. Pactul de Stabilitate își propune să sprijine reforma instituțională în statele Europei de Sud-Est.

INIȚIATIVE DE COOPERARE CE ACTIVEAZĂ ÎN ZONĂ

În contextul problemelor prezentate ce caracterizează zona au apărut: Inițiativa Europei Centrale; Acordul Central European de Comerț Liber; Cooperarea economică a Mării

Negre; Cooperarea balcanică / Sud-Est europeană; Procesul de stabilitate și bună vecinătate în Sud-Estul Europei — Royamont; Inițiativa de Cooperare în Sud-Estul Europei.

Pactul de Stabilitate: este o inițiativă lansată de Germania în 1999, iar ulterior a fost pusă sub egida OSCE; reprezintă o modalitate prin care statele vest-europene încearcă să se implice mai mult în zonă. Are ca obiective: diminuarea și eliminarea potențialului conflictual al regiunii; sprijinirea dezvoltării unor regimuri democratice; aprofundarea cooperării regionale și transfrontaliere; crearea condițiilor pentru integrarea regiunii în structurile politice, economice și de securitate euro-atlantice. Activitatea sa este complementară cu celelalte inițiative regionale și este sprijinită de organizații internaționale ca UE, OSCE și NATO, Consiliul Europei. Proiectele sale sunt susținute de organisme financiare internaționale: FMI, BERD, Banca Mondială, OECD. Funcționează pe baza unei Mese regionale pentru Europa de Sud-est, divizată în 3 Mese de Lucru (Masa de Lucru I — pentru democrație și drepturile omului, Masa de Lucru II — pentru reconstrucție, dezvoltare și cooperare economică și Masa de Lucru III — pentru probleme de securitate).

Inițiativa de Cooperare Sud-Est Europeană (SECI): a apărut în 1996, la inițiativa ambasadorului SUA Richard Schifter; are drept scop încurajarea cooperării în spațiul balcanic, prin susținerea unor proiecte de cooperare economică și comercială de tip „transfrontalier și subregional".

Procesul reuniunilor miniștrilor apărării din Sud-Estul Europei (SEDM) a luat ființă în 1996 și propune promovarea cooperării regionale.

Forța Multinațională de Pace din Europa de Sud-Est (MPFSEE) a luat ființă în 1997 și prevedea constituirea unei forțe multinaționale cu valoare de brigadă care să îndeplinească misiuni de pace, sub egida ONU și OSCE. Are participanți din țările membre NATO și UE.

Grupul de Cooperare Navală la Marea Neagră (BLACKSEAFOR) / inițiativă lansată de Turcia în 1998. Are

ca state participante: Bulgaria, Georgia, România, Federația Rusă, Turcia, și Ucraina; fiecare participant se succede la conducere prin rotație; principalele misiuni: căutare și salvare pe mare, asistență umanitară, acțiuni contra minelor marine, operațiuni de protecția mediului;

CONSIDERAȚII PRIVIND FACTORII DE RISC LA ADRESA SECURITĂȚII ROMÂNIEI

Schimbările de la sfârșitul secolului trecut și începutul secolului actual au creat/crează o lume străbătută de tendințe contrarii, o lume mult mai complexă și eterogenă, marcată de ambiguități. Începutul secolului al XXI-lea este marcat de transformări profunde, ale mediului de securitate. Lumea devine tot mai complexă și interdependentă, iar fenomenul globalizării se afirmă tot mai mult ca fiind ireversibil.

Multiplicarea continuă a numărului de entități ce acționează pe scena globală prin afirmarea actorilor nestatali conduce la creșterea complexității procesului de luare a deciziilor în politica externă și de securitate a statelor.

Modificările induse de procesul globalizării, suprapunerea acestuia cu tendințele spre regionalizare și fragmentare, generează noi tensiuni și factori de risc. Acestor modificări trebuie să li se răspundă prin noi forme de solidaritate, capabile să gestioneze un spectru larg de tensiuni și riscuri și o gamă variată de manifestare a acestora, cum sunt: tensiunile etnice, traficul de droguri, substanțe radioactive și ființe umane, criminalitate organizată, instabilitatea politică a unor zone, reîmpărțirea unor zone de influență și altele.

Marile discrepanțe la nivelul dezvoltării economice care se accentuează tot mai mult în condițiile unor progrese tehnologice fără precedent, accesul discriminatoriu la educație și apărarea sănătății, la resurse esențiale ale vieții, la informație și cunoaștere provoacă grave crize sociale,

generează frustrări și stârnesc nemulțumiri. În condițiile globalizării economice, crizele sociale sunt însoțite, nu o dată, de crize de identitate, generatoare de violențe neașteptate.

În acest context, devine tot mai evident faptul că interesele și obiectivele de securitate ale statelor pot fi realizate prin cooperare internațională, care să se manifeste nu numai în situații limită, precum sunt cele create în urma atacului asupra SUA din 11 septembrie 2001, ci și în contextul problematic, economic, social și financiar al lumii de astăzi. Această nouă resolidarizare a statelor lumii se poate exprima în toate aceste domenii prin stabilirea unor forme de acțiune conjugată a tuturor națiunilor care împărtășesc interese și valori comune.

Interesele și obiectivele de securitate ale statelor europene nu sunt generatoare de stări conflictuale, mediul de securitate fiind influențat pozitiv de procesele de integrare europeană și euro-atlantică, de extinderea comunității statelor care împărtășesc valorile democrației și economiei de piață, de adâncire a colaborării regionale.

Riscurile apariției unei confruntări militare tradiționale pe continentul european s-au diminuat semnificativ. Totuși persistă fenomene de instabilitate și criză la nivel subregional și tendințe de fragmentare, marginalizare sau izolare a unor state. Țări din Europa Centrală, de Est și de Sud-Est se confruntă cu dificultăți economice, sociale și politice asociate procesului de tranziție spre societatea bazată pe principiile democrației și ale ecomiei de piață, care pot genera destule riscuri la adresa securității statelor din regiune.

Factorii de risc constau în acele elemente, situații sau condiții interne sau externe care pot afecta, prin natura lor, securitatea țării, generând efecte contrare sau de atingere a intereselor noastre fundamentale.

Vulnerabilitățile sunt definite astăzi ca stări de lucruri, procese sau fenomene din viața internă, care diminuează capacitatea de reacție la riscurile existente ori potențiale sau care favorizează apariția și dezvoltarea acestora.

România nu este și nu se va afla în viitorul apropiat în fața vreunei amenințări majore, de tip militar clasic, la adresa securității sale naționale. Se poate estima că, în perioada actuală, riscurile la adresa securității sunt preponderent de natură nemilitară și mai ales internă, manifestându-se în special în domeniile economic, financiar, social și ecologic. Perpetuarea și conjugarea unor vulnerabilități existente în aceste domenii pot afecta însă securitatea țării, generând efecte interdependente, difuze, multidirecționale, care impun modalități de prevenire și de acțiuni adecvate și flexibile. Neglijarea, amplificarea ori acumularea necontrolată acestor vulnerabilități pot crea instabilitate și să conducă la transformarea în riscuri la adresa securității.

Disocierea netă dintre evoluțiile din mediul intern și cel internațional este tot mai greu de făcut, în contextul acțiunii conjugate și întrepătrunderii unor procese care pot crea condiții favorabile pentru apariția, previzibilă sau imprevizibilă, a unor riscuri la adresa securității naționale. Accentuarea interdependențelor multiple dintre state, globalizarea și liberalizarea schimburilor de orice fel — de la cele comerciale la cele informaționale — fac tot mai dificilă o asemenea disociere într-un mediu globalizat, în care riscurile interne și externe se pot genera și potența în mod reciproc.

Fundalul pe care se proiectează dinamica acestor interdependențe este totuși unul pozitiv, fiind constituit de generalizarea la nivel european a spiritului de cooperare și dialog pentru consolidarea securității pe continent precum și implicarea tot mai activă a ONU, NATO, UE, OSCE și a celorlalte instituții europene ori organizații internaționale în gestionarea complexelor probleme globale de securitate și stabilitate.

Aceste caracteristici dominante ale climatului internațional reprezintă pentru statul român circumstanțe de mare importanță, care au rolul de a favoriza și de a încuraja accelerarea și finalizarea proceselor interne de reformă atât de necesare pentru îndeplinirea criteriilor de integrare europeană și euroatlantică.

Pe acest fundal, responsabilitatea fundamentală și mult sporită a statului este de a gestiona cu autoritate îndeosebi riscurile și vulnerabilitățile de natură strict internă, care influențează în mod inevitabil și poziționarea României în mediul internațional de securitate. Prin atenția acordată acestor factori interni, România poate, pe de o parte, să constituie în continuare un furnizor important de securitate regională și internațională și, pe de altă parte, să transforme îndeplinirea obiectivelor de dezvoltare economică și socială, susținută și durabilă, într-o resursă considerabilă și specifică pentru securitatea propriu-zisă a țării.

Principalii factori externi de risc la adresa securității naționale proveniți din zona adiacentă ar putea fi: posibile evoluții negative în plan subregional în domeniul democratizării, respectării drepturilor omului și a dezvoltării economice, care ar putea genera crize acute cu efecte destabilizatoare pe o arie extinsă; proliferarea armelor de distrugere în masă, a tehnologiilor și materialelor nucleare, a armamentelor și mijloacelor letale neconvenționale; proliferarea și dezvoltarea rețelelor teroriste, a crimei organizate transnaționale, a traficului ilegal de persoane, droguri, armamente și muniție, de materiale radioactive și strategice; migrația clandestină și apariția unor fluxuri masive de refugiați; acțiunile de incitare la extremism, intoleranță, separatism sau xenofobie, care pot afecta statul român, promovarea valorilor democratice; decalaje între nivelul de asigurare a securității și gradul de stabilitate a statelor din proximitatea României; limitarea accesului statului român la unele resurse și oportunități regionale importante pentru realizarea intereselor naționale.

O nouă categorie de riscuri sunt cele asimetrice neoclasice, ce pot consta în acțiuni armate și nearmate deliberate, având ca obiectiv afectarea securității naționale prin provocarea de consecințe directe sau indirecte asupra vieții economico-sociale a țării. Între riscurile de acest tip se pot enumera: terorismul politic transnațional și internațional, inclusiv sub formele sale biologice și informatice; acțiuni ce

pot atenta la siguranța sistemelor de transport intern și internațional; acțiuni individuale sau colective de accesare ilegală a sistemelor informatice; acțiunile destinate în mod premeditat afectării imaginii României în plan internațional, sub diferite forme și în împrejurări variate, cu efecte asupra credibilității și seriozității în îndeplinirea angajamentelor asumate; agresiunea economico-financiară; provocarea deliberată de catastrofe ecologice.

Dintre cele de mai sus, terorismul internațional se manifestă într-o formă acută fără precedent, prefigurând efecte multiple asupra securității statelor și stabilității internaționale în general.

În contextul în care constatăm o creștere a gradului de complexitate și de impredictibilitate al terorismului internațional, va trebui ca măsurile interne de management al crizelor să fie mai bine coordonate, sub cerința asigurării operative și eficiente a participării țării noastre la eforturile internaționale de combatere a acestei amenințări.

În concluzie, putem aprecia că reconfigurarea relațiilor dintre componentele specifice ale securității precum și înțelegerea proceselor din sfera securității mondiale și europene obligă statul român să își readapteze strategia proprie la evoluțiile mediului de securitate, integrând-o într-o viziune sistemică mai largă pentru a-și spori capabilitatea de contracarare a riscurilor și amenințărilor ce pot afecta interesele României.

CONCLUZII

Geopolitica și securitatea internațională constituie instrumente de analiză cu care se pot explica dimensiunile și natura crizelor contemporane și care, în același timp, identifică și fundamentează deciziile și acțiunile care trebuie luate pentru depășirea acestei crize de către civilizația noastră.

Securitatea internațională este un concept rezultat și ca urmare a apariției și dezvoltării unei economii mondiale globale interdependente, accentuată la sfârșit de mileniu de o mutație de esență constând în trecerea la societatea informațională globalizată.

Securitatea națională trebuie raportată la securitatea internațională, deoarece ne găsim într-un sistem global în care informația se difuzează instantaneu pe întreaga planetă, comunicațiile au devenit universale, transporturile supersonice și armele moderne planetare.

Acest raport trebuie analizat cu atât mai mult cu cât mondializarea nu a generat o lume în care națiunile interacționează în mod egal unele cu altele, indiferent de localizarea lor geografică.

Puterea militară poate deveni din ce în ce mai irelevantă în majoritatea conflictelor care au loc într-o economie globală caracterizată de o interdependență crescândă, în care statele sunt legate intre ele tot mai strâns, fiind în același timp prizoniere și beneficiare ale sistemului. În aceste condiții, marile puteri ale lumii trec de la pacte militare la zone de comerț liber.

Strategia de securitate națională trebuie să fie fundamentată de studiile și analizele geopoliticii și geostrategiei, deoarece acestea definesc măsurile necesare pentru asigurarea securității naționale, măsurile pentru instaurarea și menținerea protecției și a influenței dominației sau alte avantaje în spații de importanță strategică pentru securitatea internațională.

Tot pentru fundamentarea strategiei de securitate națională, trebuie analizată globalizarea și regionalizarea economiei mondiale, precum și internaționalizarea și interdependența financiară, deoarece acestea vin cu aspecte noi ale mijloacelor de impunere și dominare, în care nu se consideră ca necesară ocuparea efectivă a teritoriilor.

În climatul de nemulțumire generală și de dezamăgire, caracteristic acestui sfârșit de mileniu, un rol deosebit revine oamenilor politici, care trebuie să redea speranța și să

fundamenteze noua ordine mondială pentru mileniul trei, în care necunoscutele și pericolele de amenințare pentru cetățean să fie eliminate. Pentru realizarea acestui deziderat, trebuie asociată democrația cu economia de piață și integrarea în economia mondială, dar în același timp trebuie bine fundamentată și implementată o politică intervenționistă a statului, pentru a corecta dezechilibrele, deoarece contrar discursului privind liberalizarea integrală, legile pieței nu se stabilesc prin simplul joc spontan al economiei. Globalizarea se sprijină pe structuri de intervenție autoritară, ce acționează la scară mondială: „directoratul" celor șapte state cele mai industrializate (G7, devenit G8), „normele de ajustare structurală" ale F.M.I., acțiunea cu „valoare de reglare" desfășurată de Banca Mondială, dar nu reușește să facă față pericolelor globale, respectiv: criza socială mondială și degradarea mediului la nivel planetar.

Din atitudinea luată în multe ocazii, se poate vedea faptul că se dorește de către forțele internaționale, care susțin mondializarea și globalizarea economiei, diminuarea importanței conceptului de securitate națională și exacerbarea conceptului de securitate internațională. Dar statele au început, în ultimii ani, să privească securitatea nu numai ca pe o valoare importantă a vieții internaționale, ci și ca pe una națională de însemnătate crucială. Sintagma „securitate națională" devenind expresia cea mai reprezentativă pentru ideea de apărare a intereselor naționale, a fost preluată de numeroase țări care, dându-i un conținut tot mai dinamic și complex, au transformat-o într-un concept esențial pentru politica lor, atât internă cât și externă.

Practica a demonstrat că pentru orice stat interesele sale fundamentale pot fi afectate nu numai de către o agresiune militară, ci și de alte tipuri de agresiuni, precum și de numeroase pericole (amenințări sau riscuri) de natură extrem de diversă (politică, diplomatică, economică, informațională, psihologică, biologică, demografică, moral-spirituală, ecologică).

Securitatea națională exprimă gradul de satisfacere a intereselor naționale fundamentale ale unui stat, precum și ansamblul de măsuri luate în domeniile vieții sociale, în conformitate cu o concepție unitară, pentru promovarea și apărarea intereselor respective împotriva agresiunilor, a pericolelor, amenințărilor sau riscurilor de orice natură.

Securitatea națională reprezintă baza politicii generale a statului prin care se fundamentează teoretic și se îndeplinesc practic măsuri în toate domeniile de activitate (politic, diplomatic, economic, militar, cultural, științific, informațional, ecologic, sanitar, etc.), atât în timp de pace cât și în timp de război sau de criză, măsuri care să asigure promovarea intereselor naționale fundamentale și apărarea lor împotriva oricăror agresiuni și pericole.

Politica de securitate națională trebuie să realizeze un sistem integrat care să asigure corelarea activităților din domeniul securității și apărării naționale cu resursele umane, materiale, financiare și de altă natură, pe care statul trebuie să le aloce în acest scop.

La începutul celui de-al treilea mileniu, în plin proces de globalizare a activității economice internaționale și de mondializare a relațiilor diverse și complexe între statele lumii, putem afirma că abolirea existeței statelor nu este nici de conceput și nici de dorit, iar elementul fundamental al vieții politice și sociale rămâne statul-națiune.

BIBLIOGRAFIE

1. Col. prof. univ. dr. Cristian Troncotă, col. dr. Ioan Bidu, *Note de curs*, Colegiul Superior de Siguranță Națională;
2. *Strategia de Securitate Națională a României*, Monitorul Oficial nr. 822/20.12.2001;
3. A X-a Sesiune de comunicări științifice, *Securitate și societate: provocările mileniului trei* — A.N.I. — 2004;
4. Traian Liteanu, *Securitate și instituții*, Editura ANI, București, 2004;
5. George Soros, *Criza capitalismului global. Societatea deschisă în primejdie*, Polirom 1999.

6. Maria Negreponti-Delivanis, *Mondializare conspiratoare*, Editura Eficient, 2002.
7. Ion Iliescu, *Probleme globale. Creativitate*, Editura Tehnică, 1996.
8. Ion Iliescu, *Integrare și globalizare. Viziune românească*, Editura Presa Națională, 2003.
9. Zygmunt Bauman — Globalizarea și efectele ei sociale, Editura Antet
10. Dr. Ioan Bidu, *Meridiane de securitate*, Editura A.N.I., 2004.
11. Mihai Pricop, Adrian Tanțău, *Globalizarea și strategia firmei*, Editura Eficient, 2001.
12. Martin Hans-Peter, Schumann Harold, *Capcana globalizării*, Editura Economică, 1999.

AMENINȚĂRI TRANSFRONTALIERE LA ADRESA SECURITĂȚII NAȚIONALE

Lt. col. magistrat Stelea Covei

Anterior anului 1989, România, aparținând blocului socialist, se afla într-o stare de izolare politică și de stagnare economico-socială. Schimbările profunde, determinate de evenimentele din decembrie 1989, au marcat și pentru România, înscrierea pe drumul inevitabil al dezvoltării democratice a societății, al consolidării instituțiilor statului de drept, al trecerii la aplicarea principiilor economiei de piață, la respectarea drepturilor și libertăților fundamentale ale cetățenilor. Totodată, s-au creat premisele lărgirii cooperării și integrării majorității țărilor eliberate de regimuri totalitare în structurile Europene și Euroatlantice.

Pe acest fond, au apărut, s-au dezvoltat și s-au diversificat fenomene noi (rețele de crimă organizată, de trafic ilicit de droguri, de arme și explozivi, de materiale radioactive, de bunuri și persoane, terorism, etc.) care împiedică procesele pașnice de progres ale națiunilor, liniștea și siguranța cetățenilor.

În concordanță cu tendința globalizării și a acestor fenomene, ele s-au manifestat diferit, în funcție de gradul de ripostă al fiecărei țări afectate, astfel încât, s-a simțit nevoia integrării statelor în diverse structuri cu rol de coordonare și combatere a efectelor negative generate.

În acest context, opțiunea spre integrarea europeană și euro-atlantică a devenit și pentru România o prioritate care să-i confere stabilitate și un rol de combatant activ al acestor noi riscuri și amenințări.

DEFINIREA UNOR CONCEPTE

„Siguranța națională" este definită în art 1 din Legea 51/1991 privind siguranța națională a României, ca fiind „starea de legalitate, de echilibru și de stabilitate socială, economică și politică necesară existenței și dezvoltării statului național român, ca stat suveran, unitar, independent și indivizibil, menținerii ordinii de drept precum și a climatului de exercitare neîngrădită a drepturilor, libertăților și îndatoririlor fundamentale ale cetățenilor potrivit principiilor și normelor democratice statornicite prin Constituție".

În art.3 din aceeași lege, sunt enumerate (lit. a) faptele și împrejurările de fapt care sunt apreciate ca fiind amenințări la adresa valorilor sociale consacrate prin art.1.

Evoluția societății, consolidarea democrației și a instituțiilor statului de drept, respectarea plenară a drepturilor și libertăților fundamentale ale cetățenilor impun regândirea acestui concept, termenul de „securitate națională" apreciem ca fiind mai cuprinzător și corespunzător necesităților actuale privind definirea și elaborarea strategiei de securitate a României, crearea codului de cooperare și colaborare a instituțiilor abilitate pentru realizarea ei.

„Infracțiunea cu caracter transnațional" definită de art. 2 lit. c din Legea 39/2003 privind prevenirea și combaterea criminalității organizate ca fiind: orice infracțiune care, după caz:

1. este săvârșită pe teritoriul unui stat cât și în afara acestuia.

2. este săvârșită pe teritoriul unui stat dar pregătirea, planificarea, conducerea sau controlul său are loc, în tot sau în parte, pe teritoriul altui stat.

3. este săvârșită pe teritoriul unui stat de un grup infracțional organizat care desfășoară activități infracționale în două sau mai multe state.

4. este săvârșită pe teritoriul unui stat dar rezultatele acesteia se produce pe teritoriul altui stat".

În concluzie, infracțiunile transfrontaliere sunt fapte care prezintă pericol social, săvârșite cu vinovăție, prevăzute de legea penală, care au în conținutul constitutiv unul sau mai multe elemente de extraneitate: naționalitatea diferită a făptuitorilor; locul săvârșirii faptelor sau ale manifestării efectelor; (conform legii penale române,, prin „loc al săvârșirii" înțelegându-se spațiul unde s-a desfășurat activitatea infracțională, în tot sau în parte, ori locul unde s-a produs rezultatul, efectele acesteia); valorile sociale protejate.

Dacă aceste infracțiuni vizează valorile fundamentale ale României înscrise în Titlul I din Constituție, atunci dobândesc o gravitate excepțională prin pericolul major pe care-l reprezintă pentru securitatea națională.

Însă, în evoluția lor, aceste fapte extrem de periculoase, îmbracă formele diferitelor stadii de dezvoltare (vulnerabilitate, risc, amenințare, infracțiune) stadii care, printr-o adecvată direcționare a organelor cu atribuții în domeniul siguranței și securității naționale, pot fi cunoscute și contracarate, cu precădere în stadiile incipiente, până să se pună în pericol efectiv valorile sociale fundamentale.

De aceea, strategia de securitate națională trebuie să evidențieze corect, în fiecare etapă, vulnerabilitățile și riscurile, să stabilească direcțiile de acțiune ale organelor abilitate astfel încât să nu depășească stadiul de „pericol potențial" și, prin neluarea unor măsuri adecvate, să pună în pericol efectiv, valorile protejate.

„Criminalitatea organizată transfrontalieră" reprezintă unitatea indisolubilă existentă între „grupul infracțional organizat" (definit în art. 2 lit. a din Legea 39/2003, privind prevenirea și combaterea criminalității organizate ca fiind: „grupul structurat, format din trei sau mai multe persoane, care există pentru o perioadă și acționează în mod coordonat în scopul comiterii uneia sau mai multor infracțiuni grave, pentru a obține direct sau indirect, un beneficiu financiar sau alt beneficiu material„) și infracțiunile grave săvârșite

de acesta pe teritoriul unuia sau mai multor state ori concretizarea efectelor într-unul sau mai multe state.

Prin „infracțiuni grave", Legea 39/2003 înțelege infracțiunile pentru care legea prevede pedeapsa închisorii mai mare de 5 ani (minim special), exemplificând în art. 2 lit. b, 19 asemenea fapte.

În Convenția Națiunilor Unite împotriva crimei organizate transnaționale se menționează a fi: „un grup de trei sau mai multe persoane, constituit pentru o anumită perioadă, care acționează în concordanță cu scopul de a înfăptui una sau mai multe infracțiuni grave sau atacuri, pentru a obține, direct sau indirect, un beneficiu material sau financiar" fără a se circumscrie granițelor naționale.

Conform INTERPOL, crima organizată transfrontalieră reprezintă orice asociere sau grupare de persoane care se dedau la o activitate ilicită, continuă, al cărei scop principal este de a realiza profituri, fără a respecta granițele naționale.

În SUA, criminalitatea organizată transfrontalieră este privită ca o conspirație infracțională continuă, care se autoîntreține, având o structură organizatorică menținută prin frică și corupție și motivată de lăcomie sau aviditate.

În Canada este privită ca o activitate ilegală sistematică pentru putere sau profit săvârșită de o conspirație infracțională continuă, cu acțiuni și efecte în mai multe state.

În Australia este definită ca „o conspirație continuă și sistematică în scopul de a produce infracțiuni grave".

FORME DE MANIFESTARE ÎN ROMÂNIA

Deschiderea politică după 1989, deschiderea granițelor concomitent cu scăderea până la anihilarea controlului trecerii frontierei de stat, vidul legislativ pe fondul pronunțat revendicativ al unor categorii sociale au constituit premise ca, pe lângă beneficii, aceste măsuri să aducă și posibilitatea

manifestării unor situații doar intuite: diferite forme de trafic, mai mult sau mai puțin organizat în și din România.

După 1992–1993, pe teritoriul țării s-au manifestat acțiuni ale rețelelor de crimă organizată transfrontalieră în special în domenii legate de evaziune fiscală, contrabandă, migrație ilegală, spălarea și reciclarea banilor, traficul ilegal de droguri, falsificarea de monedă, traficul de autoturisme de lux furate din Occident care erau indighizate prin falsificarea actelor de proprietate.

În perioada evocată criminalitatea organizată s-a manifestat, cu predilecție în domeniile: *social* (migrație ilegală de persoane, prostituție, trafic ilegal de droguri); *financiar-bancar* (creditări ilegale, deturnări de fonduri, operațiuni de spălare de bani angrenându-se inclusiv instituțiile de profil); *comercial-vama* (operațiuni ilegale cu alcool, cafea, țigări, produse electronice, produse agroalimentare, materii prime).

Succesele repurtate în această perioadă au făcut posibilă expansiunea activităților rețelelor de crimă organizată, permanentizarea unor tipuri de activități ce s-au dovedit a fi rentabile desfășurate de rețele de tip mafiot de sorginte arabă, turcă, chineză, rusă și ucraineană, toate pe fondul unei reacții timide a organelor abilitate și a unui vid legislativ sau unei legislații desuete.

Această poliferarea fost posibilă datorită:

- prezenței numeroase și active pe teritoriul național a cetățenilor de origine arabă (sirieni, irakieni, iranieni, libanezi), kurdă, turcă, semnalați cu intense activități infracționale specifice infracționalității economico-financiare, structurați și organizați sub acoperirea unor activități comerciale legale. În acest caz, banii proveniți din cele mai diverse activități au fost spălați și investiți în activități legale ori scoși din țară ilegal creindu-se premisele apariției și dezvoltării nemărginite a economiei subterane, prin conjugarea eforturilor cu elemente autohtone, ajungându-se la împăr-

țirea domeniilor de activitate, nu de puține ori, prin acțiuni de o violență deosebită ori prin acte de corupție:

- existenței mai multor zeci de mii de cetățeni chinezi pe teritoriul țării, o parte însemnată dovedindu-se că sunt autorii ori implicați în desfășurarea unor fapte penale grave, victime fiindu-le în special conaționali.

Sub aparența unor activități comerciale ori sub paravanul unor firme fantomă s-au implicat în activitățiii specifice crimei organizate (trafic de stupefiante, prostituție, șantaj, tâlhării, sechestrări de bunuri și persoane) prin mijloace și metode tipic mafiote de grupări conaționale.

- penetrarea unor sfere ale activității interne de către rețele din Rusia, Ucraina și alte state din spațiul ex-sovietic, care, sub acoperirea unor activități comerciale ale unor firme din Republica Moldova, prin metode ilicite controlează activitatea unor firme românești în spațiul C.S.I. Specific acestora este că sunt constituite sau controlate de foști militari, mijloacele lor de acțiune fiind de o violență extremă iar implicarea în traficul ilegal de persoane din țările asiatice, de droguri, de arme și materiale strategice fiind deseori pusă în evidență de organele abilitate.

TRĂSĂTURILE GENERALE ȘI SPECIFICE ALE REȚELELOR CRIMEI ORGANIZATE TRANSFRONTALIERE

Deoarece pentru fenomenul crimei organizate nu există o definiție unanim acceptată, din analiza cazuisticii în domeniu s-au desprins o serie de elemente definitorii ce caracterizează organizarea, funcționarea și trăsăturile rețelelor criminale și care, conturează acest fenomen.

Elementul etnic este un factor fundamental în geneza unei rețele criminale transfrontaliere și care explică puterea unor organizații criminale internaționale formate din asiatici, chinezi, italieni, japonezi, ruși, vietnamiezi. Dezvoltarea

acestora și conlucrarea lor în diverse domenii de acțiune au făcut ca elementul etnic să fie specific organului de comandă, iar nivelul execuției nemaifiind un criteriu absolut.

Structura, bine definită și articulată atât pe verticală cât și pe orizontală, conferă unitate de acțiune, coerență, suplețe și tenacitate în definirea obiectivelor, a mijloacelor și metodelor pentru atingerea țelurilor propuse.

Sunt cel puțin trei nivele ierarhice de comandă și de execuție care respectă ierarhia, specializarea și compartimentarea activității:

- nucleul sau cupola! comanda
- locotenenții! stabiliți prin legături de rudenie, dup ăo verificare draconică a loialității față de cupolă.
- coordonatorii activităților ilegale și executanții acestora care sunt dependenți de profilul obținut; alături de aceștia coexistă, deseori fără a se cunoaște reciproc, executanții sarcinilor legale care au veleități de promovare în cadrul structurii.

Cupola este elementul de coeziune și comandă al rețelei, impus prin reguli stricte și deseori prin teroare; cine nu-l respectă conform normelor interne este aspru pedepsit, deseori eliminat fizic.

Alte trăsături și caracteristici ale crimei organizate transfrontaliere sunt: preponderența mijloacelor ilegale folosite; caracterul transfrontalier al activităților și frecventa conlucrare cu entități similare străine ori cu organizații teroriste; nivelul ridicat de recurgere la violență și/sau corupție pentru realizarea scopurilor; capacitatea de a penetra sau influența mediul politic; implicarea activă în activități ilegale ale căror profituri sunt reinvestite în economia reală, influențând climatul politic, economic și social de pe un anumit teritoriu; legături și înțelegeri cu organe ale statului gazdă.

Din enumerarea trăsăturilor de mai sus, se desprinde pericolul social major la adresa securității statelor al căror teritoriu este folosit pentru acțiune. Sub acest aspect, pot fi enumerate exemple de acțiune a unui stat împotriva unor

interese ale altui stat prin intermediul rețelelor crimei organizate transfrontaliere sau imaginate scenarii în cadrul cărora, prin aceste rețele și prin legăturile și înțelegerile cu organe dintr-un anumit stat, acestea vor acționa într-un scop contrar intereselor naționale.

EXEMPLE ALE UNOR REȚELE, CU EVIDENȚIEREA DOMENIILOR DE ACTIVITATE

Sunt cunoscute două tipuri: mafiile și rețelele specializate ale crimei organizate, diferențiate după influența asupra vieții sociale, economice și politice ale Mafiei în teritoriul natal. Ambelor le este caracteristică dorința unui profit rapid, cât mai mare și prin orice mijloace.

Mafia italiană. La sfârșitul anului 1990, Cosa Nostra număra aproximativ 5500 membri, Camorra napolitana circa 7000 iar N'Dragbeta calabreză 5000 membri. Apartenența la Mafie se dobândește prin naștere, căsătorie sau prin intermediul rudelor ori prietenilor apropiați.

Sunt inițiați ca frați, indiferent de originea națională, inițial ca ucenic sub atenta observație a unui membru cu drepturi depline. În această perioadă asimilează regulile, participă la o sumedenie de acțiuni ilegale, graduale ca gravitate, trecerea lor și implicarea lui necondiționată fiind dovada că ucenicul merită primit în organizație. Practic, dobândește profilul girantului său cu care devine partener după primire, dobândind drepturile, privilegiile, obligațiile și protecția familiei mafiote de care se desparte doar prin moarte.

Organizația are un cod de legământ („*omerta*" — *tăcere nobilă*) care încălcat atrage moartea celui în cauză. Familiile mafiote au în frunte un „cap" căruia i se spune „naș", asistat de un „subcapo" și „consigliere". Aceștia, în special consilierul, fac legătura cu locotenenții, cărora le transmit

ordinele nașului. Locotenenții organizează actul criminal propriu-zis, executat de „soldații" organizați în „regiune".

Mafia se deosebește de celelalte entități ale crimei organizate prin dorința și capacitatea ei de a influența și controla activități sociale economice și politice pe raza unui anumit teritoriu datorită legăturilor pe care le realizează prin corupție și/sau violență asupra funcționarilor publici cu rol în sistemul decizional de stat. Această „simbioză" creează premisele sporirii exponențiale ale veniturilor și puterii Mafiei, care, în situația întâlnirii unor oponenți printre funcționarii publici, aceștia sunt fie corupți fie eliminați fizic.

De aceea, în perioada 1970–1980, statul italian a organizat o ripostă importantă prin instituțiile sale determinând orientarea acțiunilor Mafiei italiene în unele țări foste comuniste și în câteva țări africane.

Mafia din SUA s-a format în primele decenii ale colonizării, inițial ca o prelungire a Mafiei italiene, penetrând viața politică, economică și socială din noile metropole americane. Activitatea ei a cunoscut unele adoptări, în sensul că s-a renunțat la unele semne simbolice în ritualul de inițiere iar consilierii, din ce în ce mai instruiți, au devenit principalii avocați ai familiei. Astfel ei aveau rolul deosebit de a orienta activitățile pentru a se specula la maximum imperfecțiunile legislative.

Domeniile de activitate erau diverse de la traficul de băuturi alcoolice și tutun, până la traficul de droguri, prostituție, jocuri de noroc, taxe de protecție, adică tot ceea ce aducea profituri mari și imediate.

Cartelurile columbiene sunt implicate în special în traficul de cocaină, contribuind formele de producție din Columbia, Peru, Brazilia și Ecuador, unde sunt cultivate circa 40.000 ha, producția exportată situându-se la 500 t (90% din producția mondială). În ultima perioadă, s-au implicat și în traficul de heroină, culturile de opiacee întinzându-se pe 20.000 ha și asigurând 45% din producția mondială.

Organizarea cartelurilor columbiene este asemănătoare: șeful cartelului; grupul oamenilor de încredere; nivelele inferioare, toate realizând o structură modulară, compartimentată și verticalizată, cu posibilitatea continuării activității chiar dacă unele componente sunt anihilate de forțele statale sau de grupuri rivale.

Cele mai importante au preluat numele localității unde își au sediul central și au o structură piramidală, formată din mai multe grupuri autonome, care controlează absolut regiunea: Medellin, Cali, Canca.

Caracteristica acestora rezidă din implicarea în economia subterană a regiunii controlate și exclusivitatea asupra tuturor operațiunilor legale, de asemenea violența extremă a acestor grupări a făcut ca guvernele din regiune să creeze structuri militariste comune de luptă împotriva culturilor de substanțe narcotice cu un important sprijin logistic din partea SUA, care constituie o principală piață de desfacere alături de Canada, Mexic și Țările de Jos.

Crima organizată rusă are o structură complexă: pe plan intern similară unei organizații de tip mafiot iar în străinătate are trăsături specifice rețelei de crimă organizată transfrontalieră specializată pe diverse tipuri de infracțiuni. S-a format după anii '90, în contextul destrămării sistemului socialist de organizare socială, de proprietate și de economie, cu scopul obținerii unor relații speciale cu reprezentanții puterii și cu funcționarii care gestionau întreprinderile și sistemul financiar. S-a ajuns ca, prin diverse „inginerii financiare" să acumuleze proprietăți importante, să patroneze economia subterană, să maximizeze profitul în detrimentul populației care a ajuns la o pauperizare continuă și accentuată.

Se apreciază că fie pe teritoriul fostei URSS funcționează spre 5800 angajați, circa 200 având ramificații internaționale, cu activități ilegale axate pe: trafic de droguri, trafic ilegal de arme, materiale radioactive și unele materiale cu dublă utilizare, migrația ilegală de bunuri și persoane, trafic

de organe umane, trafic de femei exploatate pentru prostituție în Europa, Israel și Orientul mijlociu, crimă la comandă, spălarea banilor, implicarea în activități legale prin cumpărarea de imobile în toată Europa de Vest, investiții imobiliare pe piețe aflate la început, asumarea rolului de investitori srategici pentru firme controlate,etc.

Pe teritoriul CSI nu există o structură mafiotă de tip piramidal și centralizată sub o conducere unică (tip Mafia italiană) însă organizarea pe criterii etnice, care controlează absolut un teritoriu, o apropie pe aceasta. Astfel, cele mai importante rețele sunt controlate de: armenii — specializați în taxe de protecție în domeniul comercial; daghestanii — trafic de arme, droguri, valută; azerii — controlul comerțului cu fructe la Moscova și trafic ilegal de droguri, mai ales droguri sintetice; cecenii — acțiuni violente tip racket, prostituție, trefic de droguri, acte de corupție; ucrainienii — trafic de droguri ușoare, de autoturisme de lux furate; rușii — trafic de cocaină, prostituție, trafic de materiale strategice, arme.

Crima organizată chineză reprezintă un fenomen vechi și diversificat. Cele mai cunoscute organizații criminale constituite pe principiul sindicatului crimei sunt: Triadele, Grupul 14 K, Uniunea Bamboo, Born to kill, Dai huen jai, Flying Dragons etc. *Triadele* (care conferă și titulatura crimei organizate chineze) datează din secolul al XVII-lea și în prezent s-au răspândit și funcționează în toată lumea, înlesnite de migrația masivă chineză și actele de corupție practicate pe scară largă. Au o structură tip plasă speculând organizarea în comunități, adevărate orășele în orașele care le-au adoptat, dominate de legi proprii, penetrarea lor de către autorități fiind practic nulă. Sunt implicate în traficul ilegal de droguri, jocurile de noroc, prostituție, trafic ilegal de persoane, evaziune fiscală, contrabandă, spălarea banilor.

Organizarea rețelelor are o ierarhie cu mai multe nivele de conducere, fiecare rang definit de un titlu și un număr, conferite în baza unui ritual. Liderul, „șeful Dragon" are 489;

„ofițerii susținători" au numărul 438; „soldații" au numărul 49. Relațiile dintre ei au la bază legătura dintre „fratele mai mic" și „fratele mai mare" în cadrul căreia, primii sunt datori să ofere loialitate, ajutor și bani în schimbul protecției și sfaturilor.

Se apreciază la 80.000 numărul membrilor Triadelor, cele mai cunoscute fiind „Wo" și „14K" implicate în traficul mondial de droguri, cu control total în Hong-Kong, Taiwan și Singapore.

Yacuza japoneză își are originile în secolul al XIV-lea, caracterul secret și activitățile desfășurate îndepărtând-o de la țelul inițial: protecția proscrișilor de pe proprietățile feudale. Numele provine de la jocul de cărți Sammai Kamta, a căror combinație (8-ya, 9-ku, 3-sa) dă 20 de puncte. Aceste rețele au o structură piramidală rigidă: părintele (șeful) — oyaban; câțiva discipoli, succesori, copii (kobun); membrii familiei (gumi).

Cea mai importantă familie — *yamaguchi* — are circa 10.000 de membrii.

Se estimează că Yaccuza este compusă din 150 de familii cu 220.000 membrii și-și exercită influența în multe domenii de activitate prin acte de violență și/sau acte de corupție. Este prezentă în jocuri de noroc, cămătă, taxe de protecție, trafic de droguri. În străinătate acționează pe coasta de vest a SUA, în Hawai, Hong-Kong, Bankok, Seul, Africa de Sud-Est, Australia, fiind implicată în reciclarea fluxurilor de capital obținut ilegal în economia oficială, utilizarea firmelor fantomă din diverse activități pentru obținerea creditelor care nu vor mai fi niciodată returnate. Acestea sunt posibile prin atragerea unor importanți oficiali prin acte de corupție, prin lacunele legislative oferite (spre exemplu, la Tokyo, o firmă se poate înființa ca un capitol social de 100 yeni — 1 USD).

MĂSURI DE PREVENIRE ȘI CONTRACARARE A AMENINȚĂRILOR ȘI INFRACȚIUNILOR TRANSFRONTALIERE ÎN ROMÂNIA

Evoluția legislației românești[59] în domeniu, dincolo de armonizarea sa cu legislația europeană[60] în procesele și programele de preaderare la Uniunea Europeană, constituie barometrul apariției, dezvoltării și transformării vulnerabilităților și riscurilor în amenințări la adresa siguranței naționale și ale acestora în fapte cu caracter penal pentru a căror pedepsire a fost necesar să fi creat sau îmbogățit un cadru legislativ adecvat.

——— [59] Constituția României — stabilirea cadrului legislativ general privind respectarea plenară a drepturilor și libertăților fundamentale ale omului; Legea 87/1994 — privind combaterea evaziunii fiscale; Legea 141/1997 — privind Codul Vamal al României; Legea 2/1998 — privind prelevarea și transferul de țesuturi și organe umane; Legea 78/2000 — pentru prevenirea, descoperirea și sancționarea faptelor de corupție (art 5, art 6, art 10 — art 12); Legea 143/2000 — privind combaterea traficului și consumului ilicit de droguri (art 2 — art 12); Ordonanța de Urgență a Guvernului nr 141/2001 pentru sancționarea unor fapte de terorism și a unor fapte de încălcare a ordinii publice (art 1 — art 5); Legea 678/2001 — privind combaterea traficului ilegal de persoane (art 12 — art 15); Legea 656/2002 — pentru prevenirea și sancționarea spălării banilor (art 23 — art 24); Legea 39/2003 — privind prevenirea și combaterea criminalității organizate (art 7, art 8, art 10); Codul Penal al României.

[60] Declarația Universală a Drepturilor Omului, adoptată în 1948; Convenția Europeană a Drepturilor Omului și a Libertăților Fundamentale, adoptată în 1950 (interzicerea sclaviei și a muncii forțate; interzicerea tratamentelor inumane și degradante); Convenția Națiunilor Unite de Eliminare a tuturor formelor de Discriminare împotriva Femeilor (1979- interzicerea traficului de femei); Convenția Națiunilor Unite privind Drepturile Copilului (1990 — interzicerea traficului de copii); Convenția Națiunilor Unite împotriva Crimei Organizate Transfrontaliere notificată de România prin Legea 565/2002; Protocolul Națiunilor Unite pentru Prevenirea, Combaterea și Pedepsirea traficului de persoane, în special femei și copii (2000); Decizia Consiliului Europei privind combaterea traficului de persoane (2002); Decizia Consiliului Europei privind combaterea exploatării sexuale a copiilor și a pornografiei infantile (2003).

Astfel, primele măsuri post revoluționare au vizat crearea cadrului propice afirmării principiilor democrației, ale economiei de piață și ale pluralismului politic. În acest sens au apărut: Legea 51/1991 privind siguranța națională a României, Legile asigurării trecerii de la economia centralizată la economia de piață (Legea 12/1990 privind protejarea populației împotriva unor activități comerciale ilicite; Legea 15/1990 privind organizarea unităților economice de stat în societăți comerciale și regii autonome; Legea 26/1990 privind registrul comerțului; Legea 31/1990 privind societățile comerciale; Decretul lege 54/1990 privind organizarea și desfășurarea unor activități economice pe baza liberei inițiative; Legea 21/1991 privind impozitul pe profit; etc).

Toate aceste măsuri au avut meritul de a se constitui într-o ripostă a statului în contracararea unor fenomene care prezentau pericol pentru dezvoltarea economiei și independenței societății.

Pe măsura diversificării formelor de acțiune a unor grupuri criminale, chiar transfrontaliere, au apărut acte normative cu rolul de a combate, prin măsuri punitive, fenomene aflate într-un anumit stadiu de evoluție și care riscau a deveni pericol iminente privind valorile constituționale.

Astfel au fost elaborate Legea 35/1991 privind regimul investițiilor străine; Legea 82/1991 privind contabilitatea firmelor; Legea 87/1994 privind combaterea evaziunii fiscale; Legea 141/1997 privind Codul Vamal al României; Legea 21/1999 privind prevenirea și combaterea spălării banilor (modificată și completată prin Legea 656/2002); Legea 78/2000 privind prevenirea, descoperirea și sancționarea faptelor de corupție; Legea 143/2000 privind combaterea traficului și consumului ilicit de droguri; Legea 78/2001 privind combaterea traficului ilegal de persoane; Legea 39/2003 privind prevenirea și combaterea criminalității organizate.

Dincolo de măsurile legislative enunțate, s-a creat cadrul organizării și funcționării serviciilor speciale cu rol în prevenirea, descoperirea și culegerea de informații privind amenințările la adresa siguranței naționale precum și a

conlucrării și cooperării dintre aceștia pentru realizarea sarcinilor specifice.

În paralel, au apărut și instituții noi cu rol important în combaterea infracțiunilor transfrontaliere (Oficiul Național pentru Prevenirea și Combaterea spălării banilor; Brigada de Combatere a Crimei Organizate; Brigada de Combatere a Criminalității Economico-Financiare, ambele în cadrul Inspectoratului General al Poliției Române; Secții similare în cadrul Ministerului Public; Parchetul Național Anticorupție).

Pe plan european, România face parte din sistemul Poliților Europene (EUROPOL) și din sistemele regionale de luptă împotriva crimei organizate și a traficului ilicit de droguri (Centrul SECI).

Pentru combaterea eficientă a infracționalității transfrontaliere, prin Decizia Consiliului Europei din 28 Februarie 2002 a fost creat EUROJUST — ul, organism european de cooperare judiciară în materie penală.

Acestuia i-au fost stabilite ca obiective: ameliorarea coordonării între autoritățile judiciare competente ale statelor membre privind desfășurarea anchetelor și urmării penale precum și pentru punerea în aplicare a asistenței judiciare internaționale și executarea cererilor de extrădare; susținerea autoritățile judiciare competente din statele membre în scopul eficientizării efective a anchetelor și urmăririi penale.

COMPETENȚA EUROJUST

Competența materială este acoperită de toate infracțiunile prevăzute în art 2 din Convenția Europol din 26/07/1995: traficul de droguri; taficul de persoane; terorismul; traficul de autoturisme furate; traficul cu substanțe radioactive și nucleare; falsificarea de bani și altor mijloace de plată; în

situația în care există structuri criminale organizate și sunt afectate doua sau mai multe state.

În baza Hotărârii Consiliului Europei din 06/12/2002, domeniul de activitate a fost extins și la: delicte grave împotriva mediului; tâlhărie organizată; comert ilicit cu bunuri culturale; piraterie de produse; criminalitate informatică; fraudă și corupție; infracțiuni care aduc atingere intereselor financiare ale Uniunii Europene; spălarea produselor provenite din infracțiuni; criminalitate în detrimentul mediului înconjurător; oficine de propaganda rasistă; pedofilie prin folosirea noilor tehnologii; secte religioase periculoase pentru libertățile individuale.

Pe baza EUROJUST, Consiliul de Miniștrii European va putea hotărâ inițierea unei legi prin care se va constitui un Parchet European, având ca sarcini combaterea infracțiunilor grave cu dimensiuni transfrontaliere precum și a infracțiunilor care aduc atingere intereselor Uniunii Europene.

Acesta va avea competența de a cerceta, de a urmrăi și de a trimite în judecată pe cei care au săvârșit infracțiuni de competența EUROJUST, într-o scurtă colaborare cu EUROPOL.

Având în vedere că producerea unor infracțiuni poate avea efecte greu evaluabile sau reparabile, munca de prevenire desfășurate de organele abilitate trebuie să fie amplă, precis orientată și desfășurată, într-o coordonare și colaborare perfectă, astfel încât vulnerabilitățile și riscurile la adresa securității naționale conținute de strategiile elaborate să nu evolueze către amenințări sau fapte cu caracter penal.

TERORISMUL — RISC DE SECURITATE GLOBALĂ

Colgiu Doru

„Aveați de ales între război și dezonorare:
ați ales dezonorarea și veți avea parte și de război".

Winston Churchill

Dezbaterile privind terorismul și combaterea lui au avut loc, în general, în mod izolat până la 11 septembrie 2001. Aceasta datorită faptului că terorismul a fost adesea tratat în termeni emotivi, care au afectat direct semnul de securitate al societății, lupta împotriva terorismului fiind frecvent văzută ca un obiectiv particularizat, rupt de interesele largi ale securității naționale.

11 Septembrie 2001, SUA și 11 Martie 2004, Madrid, au demonstrat că un grup terorist poate planifica, finanța și îndeplini un atac deosebit, având acces la tehnologie. Au demonstrat că teroriștii pot fi vecinii noștri. Au demonstrat că nu există loc pe care să nu-l poată lovi. Au demonstrat că pot exista consecințe profunde și fără precedent: folosirea terorii pentru a modifica opțiunea electoratului spaniol. Teroriștii sunt convinși că violența funcționează. Și odată învățați este greu de crezut că lecția se va limita la Spania. În mintea adepților Al Qaeda, popoare întregi dacă vor fi supuse unor măceluri oribile chiar înainte de alegeri vor putea fi manipulate ca să voteze guverne care dezaprobă intervenția avută ca formă de luptă împotriva terorismului. Amploarea și consecințele acțiunilor teroriste au arătat că lumea civilizată are un nou adversar perfid, imprevizibil și deosebit de periculos: *terorismul.*

S-a spus despre atentatul din 11 septembrie 2001de la New York că va schimba lumea, că nimic nu va mai fi la fel ca înainte de acest atentat. Asemenea afirmație a fost, fără

îndoială, marcată emoțional, dar în bună măsură este demnă de luat în seamă întrucât cel puțin atitudinea și, în linii importante, întreaga politică a Statelor Unite au luat o turnură diferită, în așa fel încât liderii americani sunt mai hotărâți decât oricând să intervină, inclusiv cu forța, peste tot în lume unde pericolul terorist sau al distrugerilor în masă este prezent, chiar dacă întâmpină o rezistență foarte serioasă din partea unor aliați tradiționali. S-a declanșat un război împotriva terorismului, care se dovedește deja extrem de dificil și probabil de durată, pentru că terorismul este generat de cauze complexe, unele ținând chiar de natura societăților moderne.

În orice caz a apărut astfel foarte pregnant pericolul terorismului extrem, practicat de rețele transnaționale dotate cu o capacitate de distrugere masivă pusă în serviciul unei ostilități fără limite față de Occident.

Prin Occident înțelegem lumea liberă și valorile democrației, o regiune de unde pornește globalizarea pozitivă, civilizatoare. Numai că aceste valori sunt tot mai mult amenințate de aspectele negative ale globalizării, printre care fenomenul terorist. Acesta reprezintă cel mai mare pericol la adresa securității și stabilității mondiale.

NOI TERMENI CE DEFINESC TERORISMUL SAU TERORISMUL PRIN ALTE MIJLOACE?

În comparație cu fenomenul terorist „clasic", evenimentele din SUA au adus modificări substanțiale în modul de organizare și desfășurare a unui atentat. Astfel, din punctul de vedere al modului de organizare, atacurile au fost îndelung plănuite (potrivit unor aprecieri, între 12 și 18 luni), au necesitat adunarea și centralizarea unui volum extrem de mare de informații, au presupus o coordonare perfectă, au necesitat conlucrarea mai multor persoane decât atentatorii propriu-ziși și au presupus o instruire prealabilă minuțioasă și de lungă durată a atentatorilor (în speță,

aceștia au învățat să piloteze avioane de linie). Se poate considera că a început o perioadă de cooperare și coordonare a terorismului internațional.

Din perspectiva modului de desfășurare, atentatele au presupus mai mulți pași (penetrarea sistemelor de alertă aeroportuare, deturnarea avioanelor, prăbușirea acestora), ceea ce a sporit riscul nereușitei acestora. Atentatele au fost multiple și s-au desfășurat cvasiconcomitent, ceea ce s-a mai întâmplat în foarte puține cazuri (atentatele din anul 1998 asupra ambasadelor SUA din Kenya și Tanzania, unele atentate din Germania etc.). Aria de cuprindere a fost mult mai mare decât în cazul unui atentat clasic, fiind vizate nu atât populația, cât mai ales simbolurile americane.

Realitatea dură a zilelor noastre, când suntem martorii exacerbării actelor teroriste, îndeamnă la reconsiderarea acestui fenomen, care constituie un important factor de risc și amenințare la adresa securității internaționale și care, iată, se poate transforma intempestiv în agresiune. Această percepție a stat, probabil, la baza unei aprecieri — devenită azi de mare actualitate — făcută de fostul secretar de stat american, doamna Madeline Albright, care afirma în urmă cu doar câțiva ani: „Războiul împotriva terorismului este războiul viitorului".

Așadar, se poate accepta ideea unui terorism nou, *neo-terorism*, care își păstrează rădăcinile vechi, dar care s-a adaptat perfect vremurilor moderne. Și aceasta deoarece, în prezent, comparativ cu secolele trecute, mijloacele și metodele de acțiune teroristă se pot obține neîngrădit. Terorismul a devenit accesibil oricui, cu condiția să dispună de un plan, de un scop sau de combinația celor două, depistarea și prevenirea acțiunilor acestuia devenind tot mai dificile.

Superterorismul se particularizează pregnant de formele clasice de terorism. Atentatele punctuale au fost înlocuite cu politici de distrugere sistematică. Superteroriștii nu mai vor să oblige autoritățile să negocieze. Sunt interesați doar de numărul de victime. Acest lucru are o dublă explicație. Prima constă în saturarea opiniei publice cu acte de violență

motivată politic. Cea de a doua explicație pentru apetența superteroriștilor pentru supraucidere, o constituie lipsa unui scop tactic precis. Lipsa unor succese politice este compensată prin provocarea de sute de victime din rândul „dușmanului".

Imaginea *superterorismului* nu ar fi completă dacă nu am ține cont de mijloacele potențiale care stau la baza suprauciderii: folosirea tehnologiilor de vârf și a armelor de nimicire în masă.

Este cert că majoritatea statelor lumii dispun de potențialul economico-militar care să le permită achiziționarea sau fabricarea de arme de nimicire în masă iar apetența folosirii acestora a fost probată de nenumărate ori pe parcursul istoriei. Din acest motiv folosirea armelor de nimicire în masă de către facțiuni sau organizații teroriste nu mai reprezintă decât coborârea de la palierul statal la cel substatal a unor arsenale cu care societatea omenească este deja obișnuită. În astfel de situații avem de-a face cu *megaterorismul* sau după expresia domnului general Ion Ștefănuț — șeful Inspectoratului pentru prevenirea și combaterea terorismului din cadrul SRI — cu „terorism prin folosirea mijloacelor de distrugere în masă".

Partenerii minori au găsit soluția de a-și achiziționa A.N.M., recurgând la factori biologici, chimici sau radiologici. Astăzi, inclusiv pe piață se găsește o gamă vastă de agenți chimici și biologici susceptibili de a cauza moartea: diverse insecticide, produse chimice industriale sau toxine puternice. Alt loc de achiziție îl constituie stocurile militare din țări aflate în criză așa cum sunt cele din spațiul ex-sovietic. Teroriștii au folosit deja agenți biologici și chimici dar cu rezultate limitate (gaz sarin — Japonia, bacili cu antrax — SUA). În ce privește *terorismul radiologic* există un caz clasic în Federația Rusă.

Accesul nelimitat la informații, considerat altădată mult prea strategic pentru a fi exploatat de publicul larg, permite acum dezvoltarea proiectelor paramilitare cu o viteză mai mare decât ritmul în care experții în antiterorism pot pre-

vede noile tendințe. Virușii care împânzesc rețelele de calculatoare pot fi oricând o armă extrem de sigură menită să anihileze un adversar sau chiar un partener recalcitrant. Cu cât o țară este mai dezvoltată din punct de vedere al tehnologiei informaționale, cu atât devine mai vulnerabilă. *Cyberterorismul* sau *cyberinsurgența* se bazează costuri relativ scăzute. Nu are spectaculozitatea bombelor dar poate crea haos. Sunt posibile multe ținte: telecomunicațiile, sistemul de electricitate, transporturile, serviciile de urgență, bănci și structuri financiare, conducte de petrol și gaze. Atu-urile sunt majore: costuri mici, asigură anonimatul agresorilor, acțiune rapidă și surprinzătoare, risc minim de localizare, zonă mare de acțiune depășind frontierele naționale.

Terorismul unimotivațional care se referă , de regulă la actele de piraterie (aeriană, navală, terestră) a renăscut la sfârșitul secolului XX. Pirații moderni sunt fie grupări locale care încearcă să scape de sărăcie prin obținerea ușoară și rapidă de mijloace financiare, fie pirați comerciali al căror scop este capturarea navelor de transport, nave vândute ulterior cu tot cu marfă, fie grupări dizidente în căutare de finanțare pentru echipament și armament. Pirații nu se bazează doar pe sprijinul comunităților din zonele în care operează. Există suspiciuni că există o strânsă relație între pirați și oficialitățile portuare.

„Mișcarea Verde" promovată de activiștii ecologiști radicali poate risca să derapeze în *ecovandalism* sau *ecoterorism*, pentru a-și impune revendicările. În ultimii 15 ani, în lumea occidentală s-a constatat o creștere îngrijorătoare a actelor teroriste comise în numele protejării mediului înconjurător. Grupările ecoteroriste urmăresc un scop bine determinat, un anume segment al vieții politice sau sociale — degradarea mediului înconjurător. Totuși nu pot fi numiți teroriști, intenția lor nu este de a intimida guverne sau companii ci doar să avertizeze și să deștepte interesul față de asemenea probleme.

Terorismul comis în numele drepturilor animalelor a apărut în urma mișcărilor antibraconaj. Apoi campania îm-

potriva sporturilor sângeroase s-a extins până la a include eliberarea animalelor folosite în laboratoare și atacarea companiilor farmaceutice sau a abatoarelor. Ei atribuie animalelor aceleași drepturi ca și oamenilor, mișcările violente au fost organizate preponderent în Marea Britanie.

Terorismul de masă sau stradal s-a intensificat și el în ultimii ani. Conferințele internaționale privind globalizarea economiei și finanțelor, întâlniri pe teme ecologice sau ale drepturilor omului, au fost supuse unei presiuni stradale din ce în ce mai accentuate, materializată prin demonstrații violente și revolte. Mișcarea antiglobalizare apărută în anii '90, a reprezentat matricea de emergență a acestor noi forme de violență motivată a activiștilor stradali. Conferințele internaționale reprezintă o platformă preferată pentru mediatizarea ideilor grupărilor și facțiunilor antiglobalizare. Violențele stradale sunt rezultatul unei planificări meticuloase și materializate de agitatori specializați și instructori profesioniști.

Conceptul de *terorism rezidual* acoperă fenomenul de încurajare a unor grupări naționaliste sau extremiste existente în teritoriile ocupate de forțe armate străine. Aceste elemente erau destinate inițial uzării forțelor de ocupație și perpetuării unui război de guerilă. Odată cu retragerea armatelor de ocupație și încetarea războiului, aceste forțe de guerilă urmau a fi dezafectate. Însă, au dovedit o importantă capacitate de autoreglare îndreptându-și ostilitatea împotriva foștilor sponsori (Franța, Anglia, Statele Unite). Primele manifestări ale terorismului rezidual au apărut în timpul războiului civil din Grecia când guerilele comuniste, foarte active în timpul războiului anti-hitlerist, dotate si instruite de britanici, au fost zdrobite de forțele armate engleze. În protectoratul Palestinei organizațiile teroriste evreiești au impus, prin atentate repetate și sângeroase, proclamarea statului Israel. Administrația franceză din Algeria a condamnat, practic, la radicalism pe naționaliștii algerieni.

COMBATEREA TERORISMULUI

Combaterea terorismului reprezintă un termen generic uzitat conceptual pentru a descrie totalitatea măsurilor antiteroriste și contrateroriste.

Antiterorismul cuprinde totalitatea măsurilor luate pentru a preveni emergența fenomenului terorist, în general, sau a unui act terorist în particular. Aceste măsuri se referă la evaluarea pericolului, întărirea plafoanelor de securitate, a obiectivelor potențial vizate, protecția personală și siguranța acțiunilor.

Contraterorismul reprezintă riposta la o acțiune teroristă produsă sau în curs de desfășurare. Cuprinde totalitatea procedurilor de ripostă tactică, investigarea atentatului, organizarea acțiunilor pe timpul crizei, suportul logistic al acțiunilor de ripostă.

Există trei nivele de combatere în cazul abordării globale la nivel de state și de comunitate internațională: politic și diplomatic, strategic și operativ.

Nivelul politic și diplomatic vizează atât problemele existente în cadrul unei țări care pot determina acte teroriste cât și metodele folosite de guvernele respective pentru a face față potențialelor amenințări ce se profilează pe plan intern și extern în acest domeniu.

Calea diplomatică se referă la legăturile și eforturile întreprinse de națiuni pentru soluționarea crizelor și problemelor internaționale care pot genera acțiuni teroriste. Aceasta se concretizează în înțelegeri diplomatice, inițierea unor standarde comune de conduită la nivel internațional, realizarea unor coaliții politico-militare capabile să țină sub control terorismul internațional.

Nivelul strategic trebuie să definească întreaga problematică a terorismului și să o supună analizei și dezbaterilor. Presupune definirea completă și coerentă a conceptelor privind securitatea și siguranța națională, elaborarea unei strategii de combatere a terorismului care să stabilească riguros aria de competență a fiecărei instituții cu atribuții pe această linie, modul de realizare a cooperării interdeparta-

mentale, naționale, regionale și internaționale. În acest sens, în consiliul suprem de apărare a țării, Președintele, Primul Ministru, directorii serviciilor românești de informații, conducerile Ministerului Administrației și Internelor și Ministerului Apărării Naționale au decis instituirea unui sistem național de alertă teroristă. S-au stabilit structura și modul în care ar putea funcționa viitorul Sistem Național de Prevenire și Combatere a Terorismului. De asemenea, la sediul Centrului de Coordonare Operativă Antiteroristă din cadrul SRI a fost deschisă o linie telefonică gratuită pentru semnalarea de către cetățeni a oricăror situații suspecte a genera acțiuni teroriste.

Centrul de Coordonare Operativă Antiteroristă din cadrul SRI are misiunea de a procesa analitic fluxurile de date și informații primite de la comunitatea informativ-operativă și de a asigura informarea curentă a tuturor structurilor din sistemul siguranței naționale, a factorilor de decizie politică și a instituțiilor care sunt ținte potențiale ale unui atac terorist. Nivelul strategic presupune și elaborarea unui set de norme, tehnici și proceduri de scădere a vulnerabilității proprii prin înlăturarea oricăror scurgeri de informații privitoare la țintele unui atac terorist, îngreunarea accesului spre acestea, reducerea posibilităților de retragere a atacatorilor.

Nivelul operativ reprezintă totalitatea măsurilor și deciziilor luate de Centrul de Coordonare Operativă Antiteroristă din cadrul SRI. Principalele activități specifice constau în organizarea ripostei propriu-zise. Acest lucru presupune trei faze: în prima fază, pe baza raportului inițial se hotărăște dacă este necesară notificarea altor forțe precum și cererile de cooperare. Faza a doua constă în stabilirea jurisdicției asupra atacului terorist. Faza a treia reprezintă trecerea la rezolvarea cu mijloace specifice a atacului terorist. Declanșarea unei crize teroriste reflectă în ultimă instanță un eșec al tuturor eforturilor de prevenire a amenințărilor teroriste, adică penetrarea principalelor inele concentrice de siguranță realizate de instituțiile statale cu atribuții în acest domeniu.

Structurile de ripostă contrateroristă, adică forțele implicate nemijlocit în rezolvarea unei crize teroriste în desfășurare reprezintă ultima resursă la care poate apela societatea în direcția eliminării unei acțiuni violente.

Neoterorismul ne demonstrează cât de vulnerabili suntem, cât de nepregătiți am fost față de amenințările nontradiționale cu care ne confruntăm astăzi și probabil mult timp de aici în colo. Societatea contemporană a arătat că încă nu este pregătită, nu dispune de strategii coerente, de o jurisdicție adecvată, de modalități eficace de acțiune și structuri profesioniste. Dar mâine, prin eforturile conjugate ale statelor lumii, ale organismelor internaționale, prin acțiuni energice și înțelepte pe multiple planuri, terorismul poate fi ținut sub control și redus ca amploare și efecte.

BIBLIOGRAFIE

Arădăvoaice, Gh., Iliescu, D., Niță, D., *Terorism, Antiterorism, Contraterorism*, Editura Antet, București 1997.

Hoffman, Bruce, *Preparing for the War on Terrorism.*

Hoffman, Bruce, *Combating Terrorism: In Search of a National Strategy.*

Bica Gh., Burduşel M.T., *Suportul financiar al terorismului internațional*, Editura Eficient, București 2001.

Arădăvoaice Gh., Naghi G., Niță D., *Sfârșitul terorismului?*, Editura Antet, Aprilie 2002, București.

Paul Vasile, *Asimetria strategică — Riscuri, amenințări și conflicte asimetrice*, Editura D.B.H., București 2001.

Postolache S., Toma Gh., Oros I., *Managementul stabilității*, editura Academiei de Înalte Studii Militare, București 2003.

Strategia de securitate națională a României, Hotărârea CSAT nr. 36 din 2002 privind Strategia națională de prevenire și combatere a terorismului.

CYBERTERORISMUL — NOI PROVOCĂRI

Alina Tonigaru

Globalizarea economiei mondiale s-a produs ca o consecință firească a conturării interdependențelor născute între state, a progresului fără precedent al revoluției informatice bazată pe calculator, a noilor tehnici și tehnologii de comunicare la distanță (sateliți de telecomunicații, fibre optice etc.). În virtutea acestei realități, multe din amenințările prezente — precum lupta împotriva terorismului și a crimei organizate, traficul de droguri, de persoane - necesită mai curând o abordare globală în detrimentul unei abordări la nivel strict național.

Cu siguranță, întreaga lume depinde în acest moment de calculatoare. Cu ajutorul acestora sunt administrate și controlate majoritatea serviciilor de importanță strategică a statelor, respectiv finanțele, aviația, comunicațiile. Aplicabilitatea computerelor se extinde și asupra medicinii sau transpor-turilor. Cu toate că există o oarecare încredere în noua tehnologie, vulnerabilitate ei reprezintă o certitudine.

În *„Computers at Risk"* (*National Research Council, National Academy Press, 1991*) se remarca faptul că infractorii moderni *„pot fura mai mult cu un calculator decât cu o armă"*. Tot astfel, *„terorismul de mâine ar putea distruge infinit mai mult cu ajutorul unei tastaturi decât cu o bombă"*.

Din 1991 și până în prezent tehnologia informațiilor a explodat, iar combinația a două mari probleme ale sfârșitului de secol XX a condus la nașterea a ceea ce în prezent numim *cyberterorism* sau *terorism informatic*.

Deoarece nu se poate aprecia cu certitudine amploarea riscurilor ce decurg din utilizarea rețelelor de Internet și a computerelor, este greu de realizat un control organizat asupra a tot ce ține de net și informatică.

S-au scurs mai bine de zece ani de când a fost editat acest studiu, iar în tot acest timp calculatorul și tehnologia informatică au cunoscut o dezvoltare fantastică și tot mai multe

persoane beneficiază în prezent de acces la computer. Riscurile ce țin de utilizarea rețelelor de Internet au crescut proporțional cu numărul utilizatorilor.

În prezent o persoană poate scrie cuiva, poate auzi, vedea, poate tranzacționa în timpi reali cu orice altă persoană de pe planetă, folosind un echipament minimal. În ziua de astăzi Internetul schimbă modul în care se muncește, modul de distracție și — în esență — stilul de viață al întregii lumi.

CYBERTERORISMUL — UN TERMEN ATIPIC

Pentru a vorbi însă de *cyberterorism* e necesară o definire preliminară a termenului în sine prin analiza componentelor sale.

Se poate vorbi de juxtapunerea a două dintre cele mai mari temeri ce au evoluat spre sfârșitul secolului XX: *cyberspațiu* și *terorismul* — temerea exacerbării violențelor asupra victimelor civile și neîncrederea în tehnologiile computerizate.

Barry Collin definea *lumea virtuală* (o altă expresie pentru *cyberspațiu*) ca fiind *„reprezentarea simbolică a informației — adevărată și virtuală în aceeași măsură, binară și metaforică — acel loc în care calculatorul programează funcțiile și efectuează operările de date"* [61].

Terorismul este un termen mult mai uzat, cu o multitudine de definiții. Una din cele mai concise este cea a Departamentului de Stat al SUA: *„violența premeditată, motivată politic perpetuată împotriva obiectivelor civile de către grupuri subnaționale sau agenți clandestini„*.

Combinarea celor două definiții ar avea ca rezultantă *cyberterorismul* care ar fi *„atacul premeditat, motivat politic împotriva informațiilor, sistemelor de calculatoare, progra-*

——— [61] *„The Future of CyberTerrorism"*, Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, 1996. http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm

melor și operărilor de date ce conduce la violențe împotriva obiectivelor civile și necombatanților, atac exercitat de grupări subnaționale sau agenți clandestini", conform definiției standard acceptată și uzată de Federal Bureau of Investigation (F.B.I.).[62]

O altă apreciere asupra *cyberterorismului* raportează acest fenomen la practici teroriste *„prin intermediul exploatării sistemelor computerizate canalizate asupra victimelor civile"*.

Ambele definiții au o aplicabilitate redusă. Pentru ca termenul de *cyberterorism* să aibă un înțeles strict trebuie să se facă diferențierea între multe tipuri de infracțiuni informatice prin intermediul cărora se realizează diverse acte de spionaj economic etc.

Cyber-atacurile pot fi de natură domestică (extrem de des întâlnite: accesarea neautorizată a site-urilor, infestarea cu diverși viruși informatici a rețelelor de calculatoare, distrugerea bazelor de date ale unor computere personale etc.) sau pot căpăta dimensiunile specifice unui atac terorist convențional.

Pe de altă parte, teroriștii pot fi caracterizați ca cyberteroriști, fie doar dacă ei se folosesc de atacuri teroriste ca să își atingă scopurile, fie dacă folosesc cyber-atacurile concomitent cu forme convenționale de terorism[63].

Cyberterorismul a devenit o reală amenințare în prezent, din mai multe motive: în primul rând, evenimentele din 11 septembrie 2001 au arătat că există indivizi care dețin mijloacele și agresivitatea necesară ca să atace SUA în interiorul granițelor sale[64]. În al doilea rând, aproape toate laturile vieții americane: finanțe, facilități industriale, administrație au devenit din ce în ce mai dependente de tehnologia compu-

[62] Dick, Ronald L., *„Cyber Terrorism and Critical Infrastructure Protection"* 24 iulie 2002, www.fbi.gov/congress/congress02/nipc072402.htm2.Id.

[63] Vatis, Michael A,.*Cyber Attacks During The War On Terrorism: A Predictive Analysis*, 22 sept.2001, Institute For Security Technology Studies At dartmouth Colleg

[64] *Ibidem*.

terizată[65]. În al treilea rând economia SUA și economiile multora din statele vestice este dependentă de tranzacțiile electronice care sunt vulnerabile atacurilor teroriste[66]. Pentru a vedea pe deplin amploarea acestei noi amenințări este necesar a fi analizate mai multe valențe ale cyberterorismului: extrem de importat este înțelegerea efectelor pe care le-ar putea produce un prezumtiv cyber-atac; trebuie identificate grupările care ar putea utiliza cyberterorismul; motivele generării unui atac informatic sunt și ele în prim planul unei analize; nu în ultimul rând este indispensabil a identifica instituțiile care sunt în măsură a fi pavăză în fața unor asemenea amenințări atipice și a contura mijloacele prin care utilizatorii de produse virtuale se pot apăra împotriva unor atacuri de asemenea natură. Mijloacele de prevenție sunt și ele un obiect de analiză pentru factorii instituționali responsabili.

POTENȚIALUL CYBERTERORISMULUI

Pentru a se putea evalua potențialul cyberterorismului, este util a concepe anumite situații ipotetice pe baza unor scenarii create de specialiști IT, care să vină în întâmpinarea unor posibile atacuri.

De asemenea, trebuie supuse unei atente analize și incidentele înregistrate până în prezent în lumea World Wide Web, incidente care ar putea constitui punctul de pornire spre ceea ce am putea numi *cyberterorism*.

Situațiile ipotetice previzionate vizează domenii precum:

---

[65] Pollitt, Mark M *„Cyberterrorism: Fact or Fancy?"* www.cs.georgetown.edudenning/infosec/pollit.html

[66] Borchgrave, Arnaud de, William H., Webster *„Cybercrime, Cyberterrorism, Cyberwarfare"* Center for Strategic and International Studies. http://www.csis.org/pubs/cyberfor.html

1. Alimentația: un posibil atac ar putea avea drept țintă copii, prin intermediul unui producător de cereale[67]. Un hacker ar putea intra în computerele care controlează proporția ingredientelor și ar putea modifica concentrația de fier de la 2% la 80%[68]. Acest fapt ar putea determina grave îmbolnăviri ale populației infantile, care ar putea culmina cu producerea de malformații[69].

2. Transport aerian — un cyberterorist poate avea drept țintă pasagerii unei linii aeriene, preluând turnul de control al unui aeroport prin accesarea computerelor tabloului de comandă[70]. Se pot adăuga informații false care pot sta la baza ghidării în spațiul aerian a aeronavei, despre viteza sau alte coordonate specifice, astfel încât controlorul aerian îi va da pilotului informații greșite, fără ca vreunul din ei să poată sesiza eroarea[71]. Aeronava se poate prăbuși sau poate intra în coliziune cu un alt avion.

3. Terorism convențional pus în scenă prin mijlocul computerelor: un terorist poate plasa mai multe bombe computerizate într-un oraș, bombe interconectate între ele[72] care se declanșează prin intermediul unui calculator. Explozia controlată prin calculator poate face ca bombele să explodeze, chiar dacă una din ele este dezamorsată.

4. sistemul bursei de valori — accesarea fără drept a sistemului burselor de valori sau burselor de mărfuri ar putea avea scopul de a genera modificări artificiale ale prețurilor acțiunilor sau diverselor produse prin introducerea de date false cu privire la capitalul companiilor, bugetul acestora etc. Acest fapt conduce la o destabilizare a pieței de capital, la creșterea neîncrederii populației în mediul de afaceri. Pe

---

[67] *Ibidem.*

[68] *Ibidem.*

[69] *Ibidem.*

[70] *Ibidem.*

[71] *Ibidem.*

[72] Collin, Barry C., *The Future of Cyber Terrorism: Where the Phisical and Virtual Worlds Converge.*

fundalul unor atare fluctuații, destabilizarea economică și colapsul pieței nu mai poate fi stopat[73].

5. industria farmaceutică — un hacker poate intra în calculatoarele unui linii de producție a unor medicamente și modifică datele privitoare la compoziția acestora, astfel încât urmările să fie din cele mai tragice.

Cyber-atacurile menționate anterior nu au avut niciodată loc și mulți specialiști consideră că hackerii vor beneficia cu greu de gradul de tehnologie sofisticată care să poată determina producerea unor asemenea incidente, însă în acest moment contează mai puțin faptul că aceste atentate nu s-au întâmplat, fiind mai important faptul că, potrivit specialiștilor, acestea pot fi posibile.

În acest mod poate fi dezvoltată latura de prevenire a unor tulburări esențiale ale vieții economice și sociale ale unei comunități prin mijlocirea rețelei de calculatoare.

Cu privire la situațiile reale cu care societatea s-a confruntat până în prezent, acestea nu pot fi în totalitate considerate ca având caracter terorist întrucât nu au existat revendicări de natură politică sau socială.

Cu toate acestea, istoria incidentelor înregistrate până în acest moment fac pe cei care contestă iminența amenințărilor informatice să poată realiza unde se va ajunge în momentul în care hackerii vor dispune de un echipament adecvat. Următoarele expemple sunt edificatoare.

În anul 1988 a fost consemnat primul incidente IT care a produs pagube deloc neglijabile: americanul Robert Morris a realizat un virus informatic care a infectat aproape 4000 de servere (un număr impresionant pentru acel timp) din cele 60 000 existente la acea dată în lume[74].

În 1989 un grup de hackeri autointitulați *The Legion off Doom* au preluat controlul asupra companiei telefonice *Bell*

[73] Brenner, Susan W. and Marc D. Goodman, *In Defense of Cyberterorism: An Argument For Anticipating Cyber-Attacks*, 2002 J.L. Tech&Pol'y1.

South.[75] Gruparea a interceptat convorbiri telefonice și a redirecționat apeluri, fără ca acest fapt să producă prejudicii majore, cu excepția încălcării flagrante a dreptului la viață privată a persoanelor.

În 1994 un alt hacker care era cunoscut sub pseudonimul de Merc a preluat controlul asupra unui server la compania *Salt River Project* și a avut posibilitatea de accesa computerelor care controlau nivelul canalelor de irigații din regiunea Phoenix — Arizona[76]. Identificarea acestuia nu a fost posibilă.

În 1996, un individ care avea legături cu o mișcare din statul Massachusets ce milita pentru supremație ariană a atacat un provider Internet radiindu-i[77] în întregime informațiile stocate. Concomitent, hackerul a încercat să transmită pe calea net-ului un mesaj de ură și rasism în întreaga lume, parte din mesajul acestui conținând amenințarea : *„Înca nu ați văzut adevăratul terorism electronic. Aceasta este o promisiune"* [78].

Sistemul de computere al turnului de control al aeroportului Worcester — Massachusets a fost dezactivat în 1997 de către un alt hacker. Prin accesarea neautorizată, cu scop premeditat, a sistemului acesta a întrerupt pentru 6 ore comunicarea turnului de control al Aeroportului Worcester cu Federal Airline Aviation. Nu au avut loc incidente majore, dar funcționarea aeroportului a fost afectată[79].

Tot în 1997 s-a produs un alt incident semnificativ: un hacker din localitatea Toborg — Suedia a blocat linia telefo-

---

[74] Lemos, Robert *„What are the Real Risks of Cyberterrorism"* 26 august 2002 http://zdnet.com.com/210+-1105-955293.html

[75] *Ibidem*,13.

[76] *Ibidem*.

[77] Denning, Dorothy E., *Cyberterorism*, 23 mai 2000, www.cs.georgetown.edu

[78] *Ibidem*, 16.

[79] Berinatto, Scott *„The truth About Cyberterrorism"* 15 martie 2002, www.cio.com/archive/031502/truth_content.html

nică de urgență 911 dintr-o regiune din vestul Floridei, producând panică în rândul populației[80].

În 1998 au avut loc intromisiuni neautorizate concertate către serverele NASA, cele ale Marinei americane și ale mai multor universități. Serverele au fost împiedicate a se conecta la rețeaua internațională, multe din computerele din rețea devenind ulterior inutilizabile[81]. Nu a fost localizată sursa atacurilor.

Department of Defense, ministerul apărării al SUA, a fost atacat în anul 1999, hackerii arătându-se interesați de această dată numai de amănunte referitoare la personalul angajat și salarii[82].

În anul 2000, în orașul Maroochy Shire din Australia un hacker a intrat în sistemul de control al unei companii de salubritate și a dat drumul la milioane de litri de ape menajere pe străzile orașului[83].

În 2001 doi studenți la cursuri postuniversitare au spart un sistem folosit de bănci și de companiile care emit cărți de credit pentru a proteja datele de identificare a clienților lor. De precizat este faptul că același sistem este folosit de ministerul de finanțe al SUA pentru a vinde obligațiuni și bonuri de valoare prin intermediul Internetului[84].

Aceste exemple demonstrează că se pot aduce prejudicii importante atât civililor, dar și guvernului sau companiilor private prin simpla utilizare a tastaturii calculatorului. Este doar o chestiune de timp până când acest tip de accidente și incidente rezultate din teribilism high-tech sau intenție ostilă insuficient conturată vor fi exploatate de adevărații teroriști care sunt în căutarea a noi și atipice metode de exprimare.

---

[80] Grossman, Mark, *Cyberterrorism"* 15 februarie 1999 www.mgrossmanlaw.com

[81] *Ibidem.*

[82] *Ibidem.*

[83] Berinatto, Scott, *loc.cit.*, 8.

[84] Pritchard Carolyn, *Cracks in the Sistem.*

ORGANIZAȚII CU POTENȚIAL CRIMINAL ÎN DOMENIUL IT

Identificarea grupărilor este importantă atât sub aspectul cunoașterii direcției din care vine amenințarea cât și din punct de vedere al conturării posibilelor revendicări. Totodată, identificarea unor asemenea organizații le face mai puțin primejdioase.

Este adevărat că este greu, dacă nu imposibil de apreciat originea unui atac terorist, cu atât mai mult a persoanelor care au declanșat un atare atac[85]. Numai în anul 2002 FBI a realizat peste 10.000 de anchete pe această temă, conform raportului acestei instituții pe anul 2002.

Departament of Justice — ministerul justiției al SUA - a anunțat că în cursul anului 1997 au fost intentate 48 de acțiuni împotriva terorismului internațional. În 2001, numărul lor a crescut la 204. Cauza acestei creșteri bruște o constituie, după cei mai mulți, conștientizarea populației asupra fenomenului terorist, dar și bugetului mai ridicat alocat FBI pentru împiedicarea activităților antiteroriste.

Cel mai cunoscut grup terorist este rețeaua Al-Queda. E probabil ca această rețea să recurgă la cyberterorism pentru a-și atinge scopurile, mai cu seamă că membrii Al-Quaeda nu s-au dat în lături de la folosirea și altor mijloace atipice de amplificare a terorii precum folosirea pe post de muniție a două avioane de pasageri. Iar dacă acestor ingrediente se mai adaugă și faptul că Al-Queda dispune de nuclee teroriste pe întreg globul, vom avea o imagine completă asupra extensiilor organizației.

The Rant Corporation a realizat în 1999 un raport referitor la *cyberterorism*[86]. Raportul susține că Al-Queda *„folosește pe scară largă tehnologia informațiilor"*[87]. De asemenea, Al-Queda a pus la punct o rețea de comunicații prin

---

[85] Vatis, Michael, *loc. cit.*, 2.

[86] Tom Reagan, *When Terrorist Turn to the Internet*, 1 iulie 1999, http://csmweb2.com

[87] *Ibidem*, 26.

intermediul Internetului concretizată prin emiterea de buletine informative electronice și e-mail-uri; unele persoane cu legături în grupare au subliniat constant importanța acordată Internetului de către această organizație[88].

O altă grupare teroristă este *Armd Islamic Group — GIA*, grup extremist islamic care acționează în Algeria și Franța. În lucrarea *„The Nation's Computerized Infrastructure is an Obvious Terrorism Target"* semnată de Esteban Parra este citată printre utilizatorii activi de Internet ca modalitate de producere sau de mijlocire a atentatelor.

Mediatizata grupare teroristă *Aum Shinrikyo* este una din devoratoarele de Internet, poate mai cu seamă datorită faptului că patria de origine este Japonia , unul din statele fanion ale IT-ului. În anul 2000 poliția japoneză a descoperit un fapt incredibil în momentul în care a realizat că unul din programele computerizate de urmărire a mașinilor folosit de instituție a fost creat de membrii Aum. Este o dovadă vie a potențialului acestei grupări care și-a extins capabilitățile și în domeniul IT.[89] Până la această descoperire, secta Aum a strâns date asupra mișcărilor tactice ale vehiculelor poliției japoneze, atât a celor declarate, cât și a celor sub acoperire.

După inițierea cercetărilor s-a descoperit că secta Aum Shinrikyo lucra în fapt ca subcontractantă pentru diverse firme de computere și a realizat astfel de *soft-uri* pentru cel puțin *80 de companii private* și *10 agenții guvernamentale*[90]. Pentru că Aum juca în rolul subcontractanților, și nu drept contractanți direcți, a fost realmente dificil ca guvernul japonez să identifice care au fost programele realizate de Aum.

Grupările fundamentaliste islamice Hamas și Hezbollah au recurs la Internet mai ales ca modalitate de propagandă. Hezbollah are creat un *site* propriu pe internet prin care își

[88] *Ibidem*.

[89] Denning, Dorothy E. *Cyberterrorism*, 23 mai 2000.

[90] *Ibidem*, 29.

promovează ideile. Hamas folosește Internetul în scop de propagandă, pentru recrutarea de adepți și pentru comunicare prin intermediul e-mail-urilor.

Pe teritoriul Statelor Unite există o multitudine de organizații extremiste rasiale care utilizează Internetul drept suport al atacurilor susținute împotriva site-urilor guvernamentale sau în scopul proferării de amenințări, multe din ele nefinalizate. Numărul acestora , raportat de Departament of Justice a crescut considerabil: în 1997 existau 147, în 1998 numărul a crescut la 167, în 1999 — 187, în 2000 — 194, iar în 2001 — 259, toate pe teritoriul SUA[91].

CAUZELE RECURGERII LA CYBERTERORISM

Cyber-atacurile sunt un mijloc atractiv de a menține o teroare electronică asupra guvernului, corporațiilor sau asupra populației. În primul rând este o modalitate mai ieftină decât orice altă modalitate tradițională. De cele mai multe ori, teroriștii nu au nevoie decât de un computer personal și de o simplă conectare telefonică. Nu e nevoie de arme, de pistoale sau bombe, atât timp cât se pot livra viruși către oricare obiectiv din lume. Și nu e nevoie de nici un mijloc de transport, atât timp cât livrarea se poate face din fotoliul de acasă.

Un alt avantaj îl constituie anonimatul sub care se poate ascunde un atentator pentru o perioadă îndelungată, rare fiind cazurile unde s-a ajuns până la identificarea sursei atacului. Lipsa barierelor fizice a oricăror frontiere, inexistența controalelor vamale face ca cyberterorismul să capete însemnătate în rândul organizațiilor extremiste. Direcționarea atacurilor către orice punct de pe glob și diversitatea

——— [91] TRAC „*A Special TRAC Report: Criminal Enforcement Against Terrorists*" — TRAC Reports, 2002, http://trac.syr.edu/tracreports/terrorism/report011203.html

țintelor îl plasează între posibilele preferințe ale teroriștilor viitorului.

Cyberterorismul poate afecta un număr imens de cetățeni, mult mai mare decât în situația folosirii metodelor tradiționale: deși nu constituie un act terorist, recenta infestare a PC-urilor de pe întregul glob cu virusul *I Love You*, face mai lesne aprecierea urmărilor unui atac cu adevărat malefic. Astfel, s-a estimat că virusul respectiv a afectat mai mult de *20 de milioane de utilizatori de net* și a creat pagube de miliarde de dolari. Datorită acestei „acoperiri" extraordinare, mediatizarea acțiunilor vine de la sine, iar în acest mod poate fi atins și ultimul scop al prezumtivilor teroriști IT.

Nu în ultimul rând, trebuie luat în considerare și numărul ridicat al publicațiilor de pe net, posturile de radio sau televiziune care emit direct de pe Internet.

Calculatoarele au un triplu rol: să stocheze informații, să le proceseze și să le comunice celor interesați. Posibilitățile crescute de manipulare a datelor pot să facă din calculatoare, în mod indirect, arme. Riscurile folosirii computerelor sunt concretizate în *accesibilitatea crescută și confidențialitatea precară.*

Accesibilitatea este determinată de posibilitatea ca o persoană autorizată să obțină informații sau să acționeze în mod specific prin intermediul computerului. Obținerea de informații poate fi limitată sau eliminată prin anumite mijloace, precum parolarea calculatorului, a anumitor date sau programe, asigurându-se în acest mod *confidențialitatea.*

Pe de altă parte, un hacker specializat poate „sparge" sistemul, iar astfel poate distruge datele stocate, programele instalate sau poate redirecționa, copia informațiile pentru ca, apoi, să le folosească în interes propriu sau în interesul unei organizații pentru care lucrează.

Barry Collin propunea un scenariu unde un hacker preia controlul asupra calculatoarelor unei linii de fabricare a unor alimente, alterând suplimentul de fier (sau alți aditivi) conținut de respectivele produse alimentare prin creșterea acestuia până la atingerea unei doze fatale. Un alt posibil scenariu

se referă la controlul traficului aerian care este aproape în totalitate computerizat. Dacă un presupus terorist reușește să controleze sistemele de la sol într-o manieră în care ar putea modifica coordonatele aeronavelor încât acestea să se ciocnească, ar rezulta cu siguranță nenumărate victime civile.

Tradiționalele atacuri teroriste presupun explozivi, arme nucleare chimice și biologice care nu sunt periculoase numai pentru victimele atacurilor, ci și pentru teroriști înșiși.

Cât privește cyberterorismul, acest risc pentru teroriști dispare atât la pregătirea, cât și la declanșarea atacurilor. Mai mult, prin intermediul calculatoarelor pot fi activate arme aflate chiar și pe un alt continent. În această modalitate *„arma digitală"* adiacentă asigură viața teroriștilor și ascunderea identității acestora. Pe lângă faptul că autorul poate fi cu greu identificat și reținut, problema cea mai mare o constituie posibilitatea scăzută de incriminare datorită legislației și jurisdicției diferite de la stat la stat.

CARACTERISTICI ALE CYBERTERORISMULUI

În luna august 1999, *Centrul de Studii pentru Terorism și Conflicte Atipice* împreună cu *Școala Postuniversitară Navală din Monterey*, California au dat publicității un raport intitulat *„Cyberterorismul: prospecții și implicații"*. Acest studiu s-a axat pe analiza modalităților de operare neautorizată prin intermediul calculatorului, ca instrument auxiliar unui act de terorism convențional. Au fost identificate în grupul de lucru constituit trei stadii ale capabilităților atacurilor teroriste informatice[92]:

– *stadiul simplu și nestructurat*: reprezintă abilitatea hackerilor de a dirija atacuri împotriva sistemelor de rețea utilizând mijloace de pătrundere create de către o altă persoană. Organizarea unor asemenea atacuri necesită o analiză superficială a obiectivului vizat.

[92] Denning, Dorothy, E. *loc. cit.*, 29.

– *stadiul avansat și structurat*: reprezintă abilitatea de a dirija atacuri sofisticate și concertate împotriva unor mai multe sisteme sau rețele prin intermediul unor mijloace create empiric de către atentatori sau mijloace preluate și parțial modificate de către aceștia. Asemenea atacuri presupun o analiză mai profundă asupra țintei avute în vedere.

– *stadiul complex și coordonat*: reprezintă abilitatea de a coordona atacuri capabile să conducă la catastrofe prin subminarea scuturilor integrate ale sistemelor și rețelelor net, incluzându-le și pe cele protejate prin criptare. De asemenea, în asemenea atacuri, hackerii sunt în măsură a crea ei înșiși instrumente complexe și sofisticate, adecvate și destinate special obiectivului fixat, urmare a unei analize profunde.

Trecând în vedere specificitatea cyberterorismului, studiile făcute până în prezent pe această temă au reținut următoarele caracteristici ca fiind determinante:

1. *Motivațiile* ce se ascund în spatele cyberterorismului sunt aceleași ca în cazurile oricăror acte teroriste. Cyberterorismul constituie o altă *„unealtă"*, la fel ca explozibilul sau armele automate.

2. Actele individuale de terorism sau cele executate de organizațiile teroriste pot fi comise *fără implicarea efectivă a autorilor* în mijlocul evenimentelor create. Este posibil ca autorii acestor acte să nu fie recrutați în cadrul organizațiilor teroriste, să nu lupte pentru o „cauză" anume, ci să facă parte dintre acei hackeri care acționează din motive exclusiv pecuniare.

3. Atacurile exercitate pe cale virtuală *nu pot fi previzionate* și nu se pot lua măsuri pentru preîntâmpinarea acestora. Este aproape imposibil să interceptezi în timp real un atac terorist declanșat prin intermediul calculatoarelor.

4. *Costurile* unor atare acte sunt mai mult decât reduse, întrucât mijlocul de comandă, respectiv calculatorul, e la îndemâna oricărei persoane iar rețelele de internet cunosc o extindere nebănuită în întreaga lume.

5. *Identificarea hackerilor* care operează în scopuri teroriste este extrem de dificilă, dacă nu imposibilă.

6. Activitățile de cercetare desfășurate în scopul găsirii unor modalități de prevenire a unor asemenea atacuri necesită coordonarea mai multor departamente și raportarea constantă la o altă formă de terorism.

Posibilele obiective selectate de către atentatori sunt caracterizate de anumiți factori pe care hackerii le au în vedere:

Vulnerabilitatea — cu cât sistemul vizat este de importanță mai mare pentru mersul zilnic al vieții, cu cât urmările accesării acestuia sunt de proporții catastrofale, iar acest sistem este mai informatizat, cu atât mai mult el este mai vulnerabil unor atacuri pe cale virtuală.

Vizibilitatea — posibilitatea unor atacuri crește atunci când obiectivul este în mijlocul unor aglomerații urbane. Pentru atentatori, sunt lipsite de interes zonele izolate întrucât efectul scontat — respectiv producerea terorii — nu poate fi atins.

Accesibilitatea — dacă ținta poate fi accesată prin intermediul Internetului, sau prin intermediul unei simple conexiuni telefonice, acest fapt o face cu mult mai atractivă pentru un hacker.

Un paradox este acela că atractivitatea țintei crește cu atât mai mult cu cât sistemul ce o protejează este mai închis, iar accesarea mai puțin facilă. Este cunoscut că protecția complexă a unui sistem este privită ca o adevărată provocare de către „cunoscători". Un exemplu tipic și amplu mediatizat de presa din întreaga lume îl constituie accesarea și infestarea site-ului oficial al NASA de către adolescenți din municipiul Iași, prima dată în cursul anului 1999, apoi în 2002.

DOMENII DE RISC

Cu fiecare zi, lumea civilă și cea militară depinde din ce în ce mai mult de infrastructură: energie, transporturi, co-

municații, finanțe. Competiția acerbă conduce la crearea unei piețe economice puternice, la fluctuarea costurilor, la automatizarea și computerizarea acestor domenii.

Legăturile și dependența noastră crescută de infrastructuri înseamnă totodată înmulțirea legăturilor și dependența noastră de sistemele computerizate, sisteme în care coexistă lumea reală și cea virtuală.

Același Barry C. Collin în lucrarea *„From Virtual Darkness: New Weapons in a Timeless Battle"* analiza punctele de convergență între lumea reală și cea virtuală, identificând interferențe de natură a conduce la eventuale dezastre în cazul unor anumite domenii predispuse la un asalt informatic de proporții ce ar putea conduce la dezastre: *alimentație și sănătate* — cu referire la tehnologiile folosite în industria alimentară și produsele farmaceutice; *infrastructură* — rețeaua de autostrăzi, drumuri și poduri de importanță strategică, căi ferate, hidrocentrale, centrale electrice și nucleare, stații de epurare a apei, conducte de gaz și clădiri; *sistemul financiar* — operațiuni interbancare, sistemul de asigurări sociale și de sănătate și chiar comerțul electronic; *transporturi* — vizează controlul traficului aerian, rețelele de transport urban și interurban, metrou; *serviciile de urgență și siguranța publică*; *comunicațiile* includ comunicațiile prin satelit, rețelele de Internet și calculatoare, cablu, radio și televiziune; *domeniile militare* și tot ceea ce ține de strategiile armate, mișcări de trupe, sateliți de telecomunicații etc.

. Cyberterorismul va cuprinde toate domeniile vulnerabile: societatea este relaționată și dependentă sistemelor formate la convergența lumii reale cu lumea virtuală. Societatea trebuie să se obișnuiască cu ideea că, atunci când se dorește expres, surfajul printre paginile web poate fi dăunător, poate genera metode mult mai periculoase și mortalitate potențială mai ridicată decât un pachet de explozibil.

. Cu mai puțin de 10 ani în urmă, imaginea stabilă a infrastructurii naționale o reprezentau căile ferate, aeriene, rețelele de apă potabilă, gaze naturale, energie electrică, rețeaua

de drumuri, baraje. Sunt sisteme fără de care nu pornește motorul vieții economice a unei comunități, iar lipsa acestora în viața zilnică a populației este de neconceput.

Acum, toată această lume reală este conectată la Internet. O persoană oarecare poate scrie, auzi, vedea sau tranzacționa în timp real cu orice altă potențială persoană de pe glob, fără a beneficia de un echipament scump. Mai mult decât atât, în prezent, Internetul este într-o continuă mișcare și comportă schimbări rapide. Orice individ cu intenție criminală și pregătire de excepție în domeniul tehnologiei informațiilor ar putea interfera și produce prejudicii considerabile.

O simplă trecere în vedere a principalelor infrastructuri (fie că sunt de uz civil sau militar) pe fundamentul cărora funcționează întreaga economie a oricărui stat de pe glob, infrastructuri ce au fost edificate de-a lungul a câtorva zeci de ani și de care sunt dependente sute de milioane de persoane, arată că oricare dintre acestea sunt extrem de nesigure în fața escaladării atacurilor informatice susținute. Mai mult decât atât, ofensivele neautorizate asupra mecanismului de control al infrastructurilor produc efecte în cascadă asupra altor domenii de activitate.

Amenințările împotriva unor infrastructuri pot viza:

Rețeaua de distribuție de gaz natural — datorită evoluției tehnicii în domeniu și în ideea economiei de fonduri, conductele de gaze naturale presurizate sunt controlate automat, cu ajutorul calculatoarelor în mai toate societățile civilizate. Automatizarea acestui sistem îl face cu atât mai vulnerabil, cu cât preluarea controlului asupra acestei rețele de conducte devine un prezumtiv obiectiv pentru teroriști, tentant din punct de vedere al urmărilor dezastruoase ce ar putea fi generate.

Sistemele de comunicații — în acest moment există o multitudine de companii independente care gestionează comunicațiile locale, cele interurbane sau intercontinentale. Iar numărul lor este în creștere progresivă, odată cu scăderea protecției sistemului. Este relativ facil pentru un hacker specializat de a pătrunde în interior și a produce căderea

liniilor telefonice. Nu trebuie a se uita de existența liniilor verzi ce asigură comunicarea în situații de urgență. Prăbușirea unor asemenea sisteme — mai ales dacă operațiunea are loc în paralel cu un atentat convențional — generează frică și amplifică teroarea la locul atentatului.

Sistemul de distribuție a energiei electrice („the grid") — este unul dintre cele mai vulnerabile sisteme ale infrastructurii oricărui stat. Exemplul edificator al colaps-ului ce ar putea avea loc la nivelul societății în situația căderii energiei electrice s-a produs nu mai devreme decât în vara anului 2003, când întreaga coastă de est a Statelor Unite ale Americii și a Canadei (care totalizează zeci de milioane de persoane) a rămas fără curent electric. Chiar dacă această criză nu a avut loc urmare a unei intenții criminale, ci doar ca efect al supraconsumului, doar faptul că a fost posibilă face ca sistemul de distribuție a energiei electrice să fie bifat pe lista posibilelor ținte ale teroriștilor. Fără curent electric, marea majoritate a industriei, a serviciilor, căile ferate, sistemul de sănătate publică sau cel financiar intră în moarte clinică.

Un alt exemplu este acela a unui grup de persoane, membre ale gherilelor IRA care, în prima jumătate a anului 1997, au încercat să atenteze la prăbușirea rețelei energetice a Marii Britanii. În același an, un protestatar din California, SUA, a accesat sistemul de distribuție a energiei electrice și a distrus echipamentul care livra electricitate la peste 2000 de familii. Tot în Statele Unite șapte state au rămas în anul 1996 fără curent electric, iar în 1997 s-a produs un incendiu de proporții uriașe, ambele incidente fiind considerate ca rezultat al unor acte de sabotaj economic.

Transporturile — sistemul transporturilor internaționale este caracterizat prin acțiune globală. El asigură deplasarea în spațiu și timp a bunurilor și persoanelor în orice punct al globului. În noile condiții ale globalizării, infrastructura transporturilor trebuie să asigure deplasarea unor mijloace de transport tot mai perfecționate la viteze tehnice și comerciale din ce în ce mai mari. Acest fapt se produce concomitent

cu informatizarea extinsă a întregului sistem. Mai mult, timpul de staționare în porturi sau pe aeroporturi este redus tot mai mult prin mecanizarea și informatizarea operațiunilor de încărcare — descărcare, prin utilizarea tehnologiilor moderne de transport (containerizare, paletizare, pachetizare), în acest mod cheltuielile totale cu transportul și transbordarea mărfurilor scăzând până la numai o treime.

Un atentat împotriva acestui sistem ar căpăta proporțiile unui dezastru, dacă o mână asasină ar interveni prin intermediul computerului ce controlează traficul și ar provoca intenționat o deraiere sau o coliziune a unor trenuri ce transportă persoane sau, la fel de grav, a unor trenuri ce transportă combustibili. Asemenea scenarii pot fi extinse și la o eventuală preluare a comenzilor transmise prin intermediul turnurilor de control ale aeroporturilor.

INTERNETUL — AVANTAJ SAU VULNERABILITATE?

Internetul nu a debutat ca un sistem civil de comunicare. La început a fost creat ca un proiect al Departament of Defense în SUA; Internetul — pe atunci ARPAnet — a fost realizat ca un mijloc de transfer al informațiilor civile și militare de-a lungul țării, pentru a o mai bună securizare a datelor.

Cu fiecare zi societatea a fost din ce în ce mai dependentă de Internet — iar acest mod de stocare a datelor, de comunicare, de informare a devenit parte integrantă a existenței tuturor, relaționând infrastructura la nivel statal și supra-statal, ecuația asimilând atât dimensiunea civilă, cât și cea militară.

La adresa securității unui sistem informatizat sau a unei rețele de calculatoare se pot concretiza amenințări a căror fațete vizează aspecte ce țin atât de defecțiuni ale echipamentelor, de erori umane, de operare deficitară, cât și de manipularea rețelei. Un aspect specific al cyber-amenințărilor îl constituie înmulțirea fără precedent a virușilor. Un

asemenea virus este, în fapt, un program creat astfel încât să poată pătrunde insidios și să distrugă parțial sau total datele stocate în memoria calculatorului, mergând până la distrugerea efectivă a PC-ului. Intrus clandestin în aplicațiile computerului, virusul este în măsură a se multiplica, invadând și alte programe din memorie sau de pe discuri; virusul poate migra spre alte calculatoare imediata apropiere a PC-ului gazdă sau spre alte destinații virtuale cu care PC-ul gazdă păstrează contactul (destinații unde, disimulându-se, reîncepe activitatea de replicare), contaminând în acest mod o multitudine de sisteme.

Virușii au *capacități de implantare* în programe neviciate, declanșând în acest mod infestarea acestora; virușii beneficiază de instrucțiuni care permit *propagarea și duplicarea* în noi programe — caracteristică a *„fazei contagioase a incubației"*[93]; virușii sunt extrem de activi, efectele pătrunderii lor neautorizate în sistem fiind din cele mai neașteptate.

Tipurile de virus sunt de o diversitate impresionantă, creatorii acestora tind în permanență la îmbunătățirea și să sporirea efectelor distructive. Cele mai cunoscute programe nocive de acest gen sunt: virușii *„logici"*, cei de tip *„cal troian"* (a căror caracteristică este aceea a deține o funcție extrem de cunoscută ce ascunde o alta nocivă prin care este inițial invadat sistemul, apoi sunt identificate numele și parola utilizatorului, iar ulterior valorificate datele, copiate și în final distruse), *„viermii — worms"*, *„bomba software"*.

Efectele virușilor[94] pleacă de la inofensive semnale sonore/grafice (Yankee Doodle, Ping-Pong) sau de la modificarea caracterelor din interiorul unui document (dBase), ajungând la disfuncționalități ale sistemelor (virusul Jerusalem), crearea de erori intempestive (Typo), inaccesi-

[93] Monica Șerbănescu, Ilie Botoș, Dumitru Zamfir, *Law& Crime.Net*, Editura Tritonic, București, 2003.

[94] *Ibidem*, p. 33.

bilitatea informațiilor (virusul Stoned) și distrugerea fișierelor (One Half).

NECESITATEA ELABORĂRII UNUI CADRU NORMATIV

Datorită vastității Internetului și extinderea acestei rețele în state care, evident, sunt caracterizate de legislații diverse, este foarte dificilă incriminarea acestor infracțiuni care pot avea loc prin intermediul utilizării calculatoarelor personale.

Eficiența acțiunilor și politicilor conturate în scopul întâmpinării acestui nou tip de criminalitate este pusă la îndoială de nesincronizarea prevederilor actelor normative ale statelor care reglementează acest segment al dezvoltării tehnologice.

Sistemele juridice din întreaga lume sunt puse să facă față acestei noi provocări, prin elaborarea unor soluții care să conducă la rezolvarea acestei probleme prin definirea clară a infracțiunilor ce decurg din folosirea abuzivă a cyber-spațiului. Importantă este și stabilirea unor norme care să determine sub ce jurisdicție intră delictul comis în acest atipic mod, știut fiind că lumea virtuală nu cunoaște aceleași frontiere delimitate în lumea fizică.

După o perioadă îndelungată în care s-a evitat o mobilizare generală a factorilor responsabili în vederea creării unui status al spațiului virtual — tocmai datorită scepticismului și ironiei cu care este și în prezent tratată amenințarea cyberterorismului — noul mileniu a debutat prin manifestarea unui interes constant de conturare a unui *„drept al Internetului"*.

Din perspectiva europeană, una din primele reglementări juridice aplicabile Internetului o constituie *Directiva 2000/31/CE a Parlamentului European din 8 iunie 2000* — act normativ care se referă în special la comerțul electronic de pe piața Uniunii Europene.

O semnificație aparte o are și semnarea la 23 noiembrie 2001, la Budapesta a *Convenției asupra Cybercriminalității* de către statele membre ale Consiliului Europei. Convenția se dorește a fi un preambul la măsurile ce urmează a fi luate la nivel național cu privire la infracțiunile ce aduc atingere confidențialității, integrității și disponibilității datelor și sistemelor informatice (acces ilegal, interceptare ilegală și fraude informatice).

Convenția asupra Cybercriminalității mai cuprinde reglementări cu privire la domeniul de aplicare a normelor, condițiile de supraveghere și conservare rapidă a datelor informatice stocate în trafic, confiscările și interceptările de date informatice, competența și cooperarea internațională, inclusiv în domeniul extrădării[95].

MĂSURI DE PREVENIRE A CYBERTERORISMULUI

Acordând credit unui recent raport al Departamentului de Apărare al SUA, în mod curent cel puțin 10 țări posedă mijloace ofesive informatice și capabilități de luptă pe plan cibernetic similare cu ale Statelor Unite. Mai mult decât atât, încă din 1996 un raport al Government Accounting Office (GAO) nominaliza un număr impresionant de 120 de state care aveau capabilități ofensivă informatice, de un nivel mai ridicat sau mai scăzut. Realitatea acestei potențiale amenințări este relatată într-un articol publicat în toamna anului 2000 în *Liberation Army Daily* — ziarul oficial al Armatei Chineze a Poporului — articol intitulat: *„Asimilarea resurselor strategice ale Internetului în cadrul Sistemului Militar, la același nivel de semnificație cu pământul, marea și aerul„*. Articolul tratează pregătirile Chinei de a realiza tehnologie informatică avansată — în scopul de a specula oportunitățile strategice ale Internetului și — de a sprijini

[95] *Ibidem.*

crearea a patru ramuri în cadrul serviciilor armate chineze care să studieze posibilitățile de atac informatic. «Biții» nu vor putea lua întrutotul locul gloanțelor și bombelor. Organizațiile teroriste convenționale, spre exeplmplu, nu vor abandona mașinile-capcană sau pachetele explozive, care s-au dovedit eficiente nu numai o dată, însă noutatea costului relativ scăzut și al riscului apreciabil mai mic al cyber-atacurilor va fi apreciată în scurt timp.

Ca putere de propagare, atacurile informatice pot genera o letalitate mult mai ridicată, în condițiile în care teroriștii le folosesc împreună cu alte arme convenționale sau dacă aceste atacuri conduc spre dezastre de proporții (căderea unui baraj). Spre exemplu, un scenariu implică detonarea unei încărcături explozive convenționale, concomitent cu lansarea unor cyber-atacuri asupra rețelei de comunicații a localității respective, în acest mod întrerupându-se posibilitatea unui dialog sau unei punți între locul incidentului și autoritățile sau serviciile care ar trebui să acorde primul ajutor. Consecințele cuprind două componente: producerea pe lângă numărul preconizat de victime a unui număr potențial mai ridicat de *«victime colaterale»* și, de asemenea, răspândirea acelei temeri, frici psihologice care poate lua valențele terorii.

Planul Național pentru Protecția Sistemului Informatic — făcut public la nivelul *Comisiei de Tehnologie, Terorism și Informații Guvernamentale* a Senatului SUA în luna februarie a anului 2000 — a identificat carențele existente la nivelul strategiilor guvernului federal cu privire la lansarea unor cyber-atacuri împotriva unor obiective de importanță națională și a relansat posibilitatea conturării de noi modalități de protecție și prevenire.

Critical Infrastructure Working Group (CIWG) și *President's Commission on Critical Infrastructure Protection (PCCIP)* — înființate prin *Ordinul 13010* și *Decizia Președintelui SUA nr.62* — sunt alte inițiative care vin în întâmpinarea amenințărilor siguranței naționale ale SUA,

amenințări care includ mai cu seamă domeniul războiului informatic.

Faptul că, la nivelul anului 2000, Președintele Statelor Unite a propus *alocarea unor sume importante de bani din buget* în vederea derulării unor programe care să identifice măsuri de prevenire și protejare a infrastructurilor împotriva atacurilor de natură informatică, vine să confirme existența unor amenințări serioase și reale.

Chiar dacă nu se va putea crea o protecție complet efectivă, majoritatea soluțiilor identificate vor fi suficiente pentru a împiedica atacuri de atare natură prin detectarea la timp ce va conduce spre eșecul acestora. Un asemenea proces este necesar a fi încurajat și extins la nivelul mai multor state, dat fiind că World Wide Web-ul se caracterizează printr-o deschidere nemaipomenită, iar protecția trebuie exercitată la majoritatea destinațiilor.

Siguranța infrastructurilor principale ale unei stat trebuie să constituie un obiectiv primordial care să se bucure de interesul factorilor decidenți ai fiecărei națiuni și care să se ridice mai presus de orice alt interes politic. În acest sens, se impune construirea unui *parteneriat între sectorul public și cel privat* în vederea atingerii acestui îndrăzneț țel.

Un pas important în această direcție îl constituie acțiunile publice ale *Oficiului Siguranței Infrastructurilor Critice (CIAO)* din SUA prin care s-a încurajat crearea *Parteneriatului pentru Siguranța Infrastructurilor Critice*, parteneriat ce include pe lângă reprezentanți ai guvernului federal și specialiști ai altor aproximativ 90 de corporații sau agenții federale care se ocupă în diverse modalități de siguranța infrastructurilor, ajungându-se în final la concluzia necesității regândirii întregii strategii de securitate a acestui domeniu.

De altfel, în scopul prevenirii și combaterii unor asemenea interferențe în sistemele de securitate ale SUA, Biroul Federal de Investigații (FBI) a angajat după septembrie 2001 un număr de peste 1000 de cyber-investigatori, iar bugetul alocat de SUA pentru securizarea infrastructurilor de interes

vital a fost în anul 2002 de 4 miliarde și jumătate de dolari[96]. La nivel guvernamental s-a decis în scopul pregătirii unor strategii aplicabile structurilor armate și de *intelligence* ale SUA, în ipoteza lansării unor asalturi cibernetice neașteptate.

Crearea acestui vast și complex sistem de rețele virtuale are la bază o fundație deloc securizată. Internetul nu a fost menit în nici un caz pentru a funcționa ca o rețea securizată, ci, dimpotrivă, *design*-ul său schematic a fost bazat pe o largă deschidere pentru a se putea facilita distribuirea, împărtășirea informațiilor printre cercetători și oameni de știință.

O altă problemă o constituie faptul că rețeaua Internet se dezvoltă cu mult mai repede decât posibilitățile societății de protejare a acesteia. În câteva cazuri, noile sisteme de rețea sunt integrate și *up-data*-te unul în completarea celuilalt, în vederea creșterii performanțelor acestora, însă se ajunge la situația renunțării la un sistem primar, dar sigur, la unul complex, însă cu potențial crescut de virusare.

Clișeul celei mai slabe verigi a lanțului nu a fost niciodată mai aplicabilă ca în acest context. În plus, **Raportul final** al **Comisiei pentru Protecția Infrastructurilor Critice** a SUA din 2002, a estimat că, la nivelul întregii populații a globului, aproximativ 19 milioane de persoane sunt amenințate a fi victime ale unui eventual cyber — atac cu urmări deosebit de grave.

SECURITATEA INFRASTRUCTURILOR VERSUS PROTEJAREA VIEȚII PRIVATE

Revoluția la nivelul tehnologiei informației a oferit o caracteristică determinantă a lumii virtuale: omniprezența. Frontul cibernetic acoperă absolut orice fațetă a vieții moderne. Impactul tehnologiei informației asupra societății a lăsat amprente profunde asupra oricărui domeniu care

[96] Green, Joshua, *The Myte of Cyberterorism*, noiembrie 2002, http://www.washingtonmonthly.com/features/2001/0211.green.html

vizează economia, calitatea vieții sau chiar securitatea națională. Din nefericire, afectarea acestui ultim domeniu reprezintă partea întunecată a acestui progres. Împreună cu recompensele progresului tehnologic apar noi riscuri și noi consecințe care trebuie mai bine analizate și gestionate de responsabilii guvernamentali.

Riscul producerii cyber-atacurilor vizează atât domenii de maximă importanță — precum existența posibilității unor *amenințări la adresa securității naționale sau vulnerabilități ale infrastructurilor* esențiale la nivel național — cât și simple operațiuni informatice sau *confidențialitatea și protejarea integrității datelor personale* (cum ar fi datele medicale, cărți de credit). Vulnerabil oricărui atac neautorizat este și mecanismul sistemului de evidență informatizată a persoanelor.

Planul Național pentru Protecția Sistemului Informatic a comportat în Statele Unite ale Americii mai multe discuții pe marginea dificultății rezolvării provocării de a asigura simultan *securitatea infrastructurilor* critice la nivel național și *menținerea intimității vieții private.*

Astfel, în Statele Unite ale Americii au fost constituite grupuri de lucru care să analizeze temeinic situația existentă și să identifice riscurile la care este supusă în prezent societatea în fața escaladării atacurilor informatice. Ceea ce s-a desprins ca primă concluzie în cadrul *Planului Național pentru Protecția Sistemelor Informatice* a fost faptul că trebuie corelată nevoia de răspuns la cyber-amenințări și menținerea sub un oarecare control al acestora cu nevoia de a menține un *echilibru constant între viață privată și securitate.*

Multe din aspecte ce țin de securitatea rețelei IT sunt înțelese eronat și dau naștere la scepticism, neîncredere și confuzie atât la nivelul simplului cetățean, cât și la nivelul responsabililor guvernamentali sau în rândul beneficiarilor din economie.

Deseori presa nu face decât să amplifice aceste probleme greșit înțelese, în loc să încerce să înțeleagă fenomenul, mai ales că trebuie încurajată orice inițiativă clară referitoare

la un dialog avansat care să dea rezultate între cetățeni, factori economici și guvern pe tema securității *World Wide Web*-ului.

Dacă aceste potențiale consecințe nu vor fi analizate și înțelese, cyber-amenințările — altădată un domeniu ce ținea de *science-fiction* — vor deveni realitate pentru fiecare dintre noi.

Societatea contemporană este dependentă de infrastructuri esențiale precum telecomunicațiile, sistemul de energie electrică, serviciile medicale, serviciile bancare și cele financiare, transporturi — infrastructuri ce vin să aducă societății un standard ridicat de viață. O caracteristică principală a întregului sistem este *interdependența infrastructurilor*, iar în cazul în care unul din domenii este victima unui cyber-atac și intră în colaps, există posibilitatea ca impactul asupra celorlalte să se producă în cascadă. Conform principiului dominoului, un simplu imbold poate dărâma un concern întreg. Pentru a întregi această problemă, autoritățile militare și cele ale justiției ar trebui să monitorizeze atacurile sau tentative neautrorizate de a accesa asemenea sisteme de importanță națională pentru a avea o imagine completă a fenomenului.

Chiar și așa, multe din persoanele responsabile rămân sceptice sau de-a dreptul ignorante în privința unor asemenea potențiale pericole. Este adevărat că e dificil a vizualiza cyber-amenințările la fel de lesne precum ar fi aprecierea dezastrelor ilustrate într-un documentar despre progromul evreilor sau despre atacul nuclear de la Hiroshima. Deseori, amenințările informatice nu pot fi luate în serios întrucât — spre exemplu — nu se poate vizualiza dezvoltarea unui cyber-atac. Chiar dacă poți fi speriat de acest tip de abstract, nu este ușor în nici un caz să fii cuprins de teroare.

Astăzi, marea majoritatea a bunurilor sunt stocate electronic, iar țintele nu mai sunt de mult de factură militară, ci sunt mai degrabă stocate in sisteme de rețele și calculatoare publice sau private. Războiul informatic se exinde și tinde să cuprindă întreaga societate. Invazia cyberspațiului este în acest moment un eveniment zilnic. Bariera unui ocean,

spre exemplu, sau o armată bine instruită sub aspect al pregătirii fizice nu mai pot fi pavăză în calea protecției teritoriului unei țări; în schimb trebuie dezvoltate și diversificate mijloacele care să conducă la reducerea riscurilor în mediul electronic care nu cunoaște frontiere.

Spectrul amenințărilor diferă de la un minor incident la un atac asupra unui fragment major de populație care nu este pregătită să discearnă cine sau ce anume a fost emitentul unui atac de asemenea factură. În plus, hakerii sunt dificil de localizat, un virus puternic (un cal troian) putându-se propaga dintr-o țară în alta, dintr-un sistem în celalalt, în timpi imperceptibili uman, de tipul nanosecundelor. Astfel, un atac inițiat din partea opusă a globului poate părea declanșat din apartamentul vecin sau, dimpotrivă. Aceste fapte se întâmplă în timp ce autoritățile statale au competențe determinate de granițele jurisdicționale ale țării, granițe stabilite în lumea fizică ce nu au relevanță asupra cyberspațiului.

În concluzie, cyberspațiul pe care ni l-am creat este construit pe fundamentul comunității globale, lipsită de secții de poliție.

În condițiile în care s-ar recurge la un control strict și aspru al traficului intens de pe net și la monitorizării terminalelor suspecte sau la ocluzionarea canalelor de comunicare de tip rețea, cu siguranță că vor exista voci care să susțină că ar fi o greșeală întrucât s-ar pune serviciile de securitate sau forțele polițienești în *poziția de a compromite drepturile cetățenești* sau *de a sacrifica dreptul la viață privată* sub argumentul forte al protecției cetățeanului. Nu este de dorit o victorie minoră cu prețul distrugerii valorilor sociale protejate: acest fapt face societatea mai puțin deschisă, mai puțin tolerantă și, nu în ultimul rând, mai puțin liberă.

Totodată, trebuie recunoscute multitudinea de avantaje generate de dezvoltarea tehnologiei informatice și, de asemenea, e necesar a înțelege că acest tip de beneficii sunt prioritare oricărui alt risc ce s-ar putea interpune în calea

progreselor industriale. Strategia de răspuns la amenințările de orice tip nu trebuie să împiedice drumul ascendent al inventicii care să conducă spre îmbunătățirea calității vieții individului. Societatea nu își permite o reacție exagerată, nu își permite să ridice prea multe ziduri reale sau virtuale. Altfel, cei care doresc îngenuncherea civilizației moderne vor câștiga în contumancie, dacă se va ajunge până într-acolo încât se va aduce ofrandă luptei împotriva terorismului drepturile și libertățile individuale care definesc principiile unei societăți democratice sănătoase.

Este posibil a se garanta securitatea infrastructurilor indispensabile — forțe motrice ale funcționării economiei unui stat — fără a compromite libertățile civile și viața privată și fără a pune lacăt Internetului? Istoria a statuat faptul că prima obligație a unui stat este aceea de a-și proteja cetățenii. Amenințările asimetrice prezente nu fac din acest principiu o excepție de la regulă. Tehnologia informațiilor, domeniul care a furnizat și va furniza în continuare avanaje imense comunității, a creat deopotrivă noi tipuri de vulnerabilități ce pot fi exploatate. Este de datoria noastră de a menține un echilibru între acoperirea acestor vulnerabilități și protejarea libertăților civile pe care societatea și le-a câștigat de-a lungul timpului.

Adesea, dezbaterile se limitează în jurul dilemei dacă securitatea și viața privată se exclud reciproc. De la bun început, este eronată premisa care elimină un factor de stabilitate în favoarea celuilalt. Constituie o certitudine faptul că menținerea unui climat de securitate poate conviețui împreună cu ocrotirea libertăților individuale. În fapt, factorii politici responsabili trebuie să prezerve convergența a acestor obiective.

La începutul anului 2000, Frank J. Cilluffo — director al *Organized Crime Project* și șef al *Task Force on Information Warfare & Information Assurance* din cadrul *Centrului pentru Studii Strategice Internaționale* al Senatului SUA declara că Silicon Valey și Washington DC trebuie ca, umăr la umăr, pe picior de egalitate, să analizeze situația creată

la nivel global și să formuleze răspunsuri limpezi referitoare la aceste noi cyber — amenințări.

Este o certitudine: viitorul nu mai e ceea ce a preconizam a fi. Cea mai sigură modalitate de a prevedea viitorul este de a-l construi prin noi înșine. Nu este necesar să fim puși în situația de a alege între securitate și protecția vieții private: putem să le avem pe ambele cu un efort consistent din partea societății.

ÎN LOC DE CONCLUZIE

În situația în care se va menține abordarea tradiționalistă în previzionarea actelor de terorism și se va răspunde mereu la întrebarea: *«Există cyber-terorism?»* cu răspunsuri superficiale de genul: *«Da, dacă există și un atentator pe nume Cyber»*, nimic nu ne va face mai vulnerabili în fața unor atacuri concertate venite pe calea *World Wide Web*. Acest tip de reacție este similară cu cea a exprimării surprinderii în fața faptului că România dispune de un serviciu antitero, deși nu a fost pusă în fața unor atentate teroriste de proporții.

Dacă factorii decidenți vor considera în continuare că, pentru a da credit unui termen ca *cyberterorismul*, trebuie ca, mai întâi, să se producă o catastrofă cu urmări considerabile pentru a justifica existența conceptului, suntem departe de a fi cu adevărat profesioniști.

Se impune cu necesitate o analiză profundă a acestui tip de amenințări și a metodelor prin care atacurile informatice pot produce efecte de natură a le include în rândul celor care sunt caracterizate de un grad ridicat de risc.

Este important ca instituțiile ce au ca obiect securitatea națională, dar și cele polițienești, să fie pregătite a interveni în cazul unor asemenea incidente, astfel încât să reușească a reduce la minim riscurile și efectele unor cyber-atacuri.

Însă, pentru ca acest lucru să devină o realitate, trebuie ca aceste instituții să conștientizeze realitatea, iminența amenințărilor informatice și amploarea dimensiunii la care

este pe cale a se dezvolta *cyberterorismul*, în acest nou mileniu al informaticii.

BIBLIOGRAFIE

National Research Council, *Computers at Risk*, National Academy Press, 1991.

Collin, Barry C., *The Future of CyberTerrorism*, Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, 1996 http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm

United States Dept. of State, *Patterns of Global Terrorism*, Washington, DC, 1996. Icove, David, et al., *Computer Crime - a crimefighter's handbook*, O'Reilly & Assoc., Sebastopole, California, 1995.

Barrett, Neil, *Digital Crime*, Kogan Page Limited, London, 1997.

Power, Richard, *Current and Future Danger*, Computer Security Institute, San Francisco, 1995.

Collin, Barry C., *The Future of CyberTerrorism*, Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, 1996 http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm

Monica Șerbănescu, Ilie Botoș, Dumitru Zamfir, *Law&Crime.Net*, Ed. Tritonic, București, 2003.

Green, Joshua, *The Myte of Cyberterorism*, noiembrie 2002, http://www.washingtonmonthly.com/features/2001/0211.green.html

Denning, Dorothy E. *Cyberterrorism*, 23 mai 2000.

Lemos, Robert, *What are the Real Risks of Cyberterrorism*, 26 august 2002, http://zdnet.com.com/210+-1105-955293.html

Borchgrave, Arnaud de, William H., Webster, *Cybercrime, Cyberterrorism, Cyberwarfare*, Center for

Strategic and International Studies. http://www.csis.org/pubs/cyberfor.html

Dick, Ronald L., *Cyber Terrorism and Critical Infrastructure Protection*, 24 iulie 2002, www.fbi.gov/congress/congress02/nipc072402.htm2.ld.

FACTORI DE RISC LA ADRESA SECURITĂȚII ROMÂNIEI. MĂSURI DE CONTRACARARE A ACESTORA ÎN PRIMUL DECENIU AL SECOLULUI XXI

Adina Simona Aprodu

Noul mediu de securitate în perioada post-război rece reclamă analiza atentă a factorilor de risc la adresa securității naționale.

Noțiunea de *factor de risc* la adresa securității naționale reprezintă, în opinia noastră, gradul de probabilitate ca anumite acte (conștiente sau inconștiente), evenimente, sau procese sociale, fenomene sau procese naturale să afecteze negativ, direct sau prin intermediul unor lanțuri de determinări cauzale de o extremă diversitate, interesele naționale ale unui stat.

Factorii de risc la adresa securității naționale trebuie căutați atât în interiorul sau exteriorul țării, cât și în planuri diferite (social sau natural, material ori spiritual, politic, economic, militar, informațional, ecologic etc.).

O definiție interesantă în legătură cu această problematică o dă Simion Boncu: „*Riscul la adresa securității naționale* implică prezența unor factori activi sau potențiali care pot afecta securitatea unui stat. *Amenințarea* vizând securitatea națională implică atât existența factorilor de risc, detectată prin perceperea unor indici specifici, cât și conturarea voinței politice de a pune în acțiune mijloacele respective pentru a leza securitatea altui stat"[97].

[97] Simion Boncu, *Securitatea europeană în schimbare. Provocări și soluții*, Editura Amco Press., p. 75.

FACTORI DE RISC EXTERNI LA ADRESA SECURITĂȚII NAȚIONALE

În rândul acestui tip de factori de risc, documentele programatice ale securității și apărării țării, precum și unele studii în domeniu menționează, printre altele: terorismul internațional; proliferarea armelor de distrugere în masă și a tehnologiilor aferente; criminalitatea organizată internațională; evoluțiile negative în plan subregional în domeniul democratizării, respectării drepturilor omului și al dezvoltarii economice; fenomenul migrației; decalajele între nivelurile de asigurare a securității și gradul de stabilitate ale statelor din proximitatea României; limitarea accesului statului român la unele resurse și oportunități regionale importante pentru realizarea intereselor naționale; subdezvoltarea; explozia demografică; criza energetică și de materii prime; criza alimentară; insuficiența resurselor de apă; modificările climatice; catastrofele ecologice; dezastrele de naturi diferite ș.a. Dintre factorii de risc externi menționați vom prezenta, succint, doar o parte.

Terorismul constituie în mod evident un factor de risc major la adresa securității oricărui stat. Groaznicele atentate din 11 septembrie 2001 din SUA, cele din 11 martie 2004 din Spania, ori acțiunile teroriste din alte puncte ale lumii (Oklahoma, Moscova, Nairobi, Istanbul, Khobar etc.) ne-au demonstrat cât de devastatoare pot fi consecințele acestui fenomen. Prin posibila utilizare a unor arme de distrugere în masă (nucleare, chimice sau biologice), terorismul reprezintă cel mai periculos fenomen pentru securitatea națiunilor. Serviciile de informații ale statului atrag atenția asupra faptului că, pe teritoriul României, în următorii ani, se vor consolida structurile active ale unor organizații teroriste străine, care vor antrena, pe lângă amenințările reprezentate de scopurile acestora, și riscurile induse de activități adiacente sau asociate cum ar fi: migrația ilegală,

traficul de droguri, de arme și muniții, de substanțe sau tehnologii supuse controlului internațional, contrabanda etc. Serviciile respective estimează că cele mai active nuclee constituite pe teritoriul țării noastre de către organizații teroriste străine care vor genera pericole, riscuri și amenințări la adresa securității naționale vor continua să fie organizațiile de esență fundamentalist-islamică („*Hezbollah*", „*Hamas*", „*Frații Musulmani*", „*Partidul Eliberării Islamice*") și alte grupări care vor acționa pentru: crearea și consolidarea unor structuri de acoperire economică, culturală, profesională sau religioasă, menite să camufleze și să faciliteze preocupările care depășesc cadrul legal; influențarea opiniei publice în vederea legitimării cauzei și acțiunii lor; dezvoltarea de structuri informative proprii; stabilirea potențialelor ținte ale unor atentate teroriste; realizarea de depozite clandestine de armament, muniții și exploziv, în vederea folosirii lor în acțiuni de tip terorist ș.a.

Proliferarea armelor de distrugere în masă este un important factor de risc extern la adresa securității naționale. Puterea explozivă totală a celor câteva zeci de mii de încărcături atomice existente este estimată a fi de 1–2 milioane de ori mai mare decât cea a bombei aruncate asupra Hiroshimei. Dacă s-ar raporta puterea totală a arsenalelor nucleare la numarul locuitorilor planetei, fiecărui om i-ar reveni, în medie, echivalentul a 15 tone de trotil. Cu toate eforturile internaționale pentru neproliferarea armelor atomice, se înregistrează, totuși, un proces periculos de difuzie a acestora spre tot mai multe țări, proces care, probabil, se va amplifica în următorii ani. Un factor de creștere a acestei difuzii este costul relativ redus al noilor tehnologii nucleare. Un motiv serios de îngrijorare este acumularea periculoasă de material fisionabil, care poate fi utilizat în scopuri distructive. Cantitatea de uraniu, produsă în lume după cel de-al doilea război mondial, care poate fi întrebuințată în sens distructiv,

este de câteva mii de tone, iar cea de plutoniu este de ordinul sutelor de tone, în condițiile în care un proiectil nuclear de artilerie, cu puterea de o kilotonă de trotil (TNT), necesită doar 75 de grame de material fisionabil. Această acumulare, asociată cu gravele deficiențe în depozitarea, mânuirea și evidența materialelor fisionabile, deficiențe manifestate îndeosebi în fosta Uniune Sovietică, dar nu numai, a alimentat o serie de fluxuri ilegale de astfel de materiale, un trafic „subteran", practicat pe scară tot mai largă. Aceste date dau o semnificație aparte atenționării făcute recent de către directorul Agenției Internaționale pentru Energie Atomică, care preciza, în ianuarie 2004, că „pericolul unui razboi nuclear nu a fost niciodată atât de mare"[98].

Menținerea subdezvoltării în lume și accentuarea unor dezechilibre economice este, de asemenea, un factor de risc la adresa secutității oricărei națiuni. în ciuda unor mari realizări economice ale omenirii din ultimele decenii, (creșterea producției mondiale de bunuri și servicii, a venitului mediu pe locuitor, scăderea ponderii populației sărace, numărul celor săraci, în cifre absolute, a crescut[99]. Subdezvoltarea rămâne, deci, un flagel caracteristic pentru numeroase țări și popoare, iar contradicția dintre statele bogate și cele sărace (*Nord-Sud*), ori între cele sărace (*Sud-Sud*), devine una din dominantele registrului marilor tensiuni internaționale. Cincimea cea mai bogată a populației se bucură de 83% din venitul mondial, în timp ce cincimea cea mai săracă utilizează doar 1,5% din acesta[100]. Cele mai

[98] „Gardianul", 27 ianuarie 2004.

[99] Département de l'informations des Nations Unies, ECOSOC, DPI/1736/POV (www.un.org/french/ecosocdev/geninfo/poverty/dpi1736f.htm, 27.12.2000).

[100] Pauvreté et développement. Persistance des déséquilibres à l'echelle mondiale, *Rapports sur les développement humain 1992–1995*, Département de l'informations des Nations Unies, DPI/1779/POV (www.un.org/french/ecosocdev/ geninfo/ poverty/dpi1779f. htm, 24.12.2000).

bogate 225 de familii din lume dispun de o avere egală cu venitul anual al celei mai sărace jumătăți a populației globului, iar averea deținută de primii trei din cei mai bogați oameni din lume depășește produsul economic anual însumat realizat de cele mai sărace 48 de țări. Aceasta în timp ce un miliard de persoane subzistă cu mai puțin de un dolar pe zi, 1,2 miliarde nu au acces la apă potabilă, 1,6 miliarde sunt analfabeți, iar 2 miliarde nu beneficiază de electricitate[101].

O sursă majoră de insecuritate o reprezintă *explozia demografică*. Statisticile în legătură cu acest domeniu sunt îngrijorătoare. Conform datelor furnizate de Fondul Națiunilor Unite pentru Populație, numărul locuitorilor Pământului, de 6 miliarde, s-a dublat din 1960 și continuă să crească cu 78 de milioane (aproape cât populația Germaniei) anual[102]. Țările în curs de dezvoltare contribuie cu 95 la sută la creșterea populației, în timp ce aceasta s-a încetinit sau s-a oprit în Europa, America de Nord și Japonia[103].

Numărul actual al *emigranților internaționali* este estimat în prezent la 175 de milioane, însemnând 3 procente din populația lumii[104]. Potrivit profesorului Viorel Roman, în viitor, dinamica demografică va duce la catastrofe sau conflicte necunoscute în trecut ca amploare; explozia demografică și viitoarele migrații constituind elemente fundamentale ale noii ordini mondiale, indiferent cum va arăta

---

[101] Lester R. Brown și Cristofer Flavin, *O nouă economie pentru un secol nou,* în *„Probleme globale ale omenirii. Starea lumii 1999"*, Editura Tehnică, București, 1999, p. 38, 39.

[102] *Etat de la population mondiale 1999. 6 milliards. L'heure du choix,* FNUAP, Fonds des Nations Unies pour la population, 1999, p. 1.

[103] *Ibidem.*

[104] Brunson McLinley, Declarație la a 37-a Sesiune a *Comisiei privind populația și* dezvoltarea spre un management mai eficient al mișcării oamenilor, New York, Martie 2004. (www.iom.int/en/PDF_Files/Other/DG_CPD_230 32004.pdf).

ea în viitorul nu prea îndepărtat[105]. În ceea ce privește România, procesul de îmbătrânire demografică, instalat la noi în urmă cu 30 de ani, continuă să progreseze, cauza principală fiind scăderea pe termen lung a natalității, ceea ce determină schimbarea structurii pe vârste a populației, creșterea ponderii bătrânilor și scăderea ponderii tinerilor. Începând din 1992, numărul morților este mai mare decât al noilor născuți, ceea ce înseamnă că populația țării este în scădere (rata sporului natural este negativă). Conform prognozelor Centrului de Cercetări Demografice din București, populația României va continua să scadă până în 2025 cu 2–2,5 milioane de oameni, iar îmbătrânirea demografică se va accentua sistematic.

Consecință firească a exploziei demografice și a subdezvoltării, *criza alimentară mondială* se adâncește în continuare. Suprafețele cultivate sunt în scădere, iar producția anuală de îngrășăminte stagnează și ea, ca urmare a atingerii nivelului de saturare. Suprafața totală irigată a început să se plafoneze, întrucât râurile și apele freatice încep să fie neîndestulătoare. Producția de pește oceanic, deși cererea pentru această resursă s-a amplificat numai în ultima jumătate de secol de patru ori, stagnează deja la un nivel care nu mai poate fi depășit.

Cercetători de la institute prestigioase de profil din SUA atrag atenția că *insuficiența surselor de apă* și distribuția inegală a acesteia are șansele să devină o sursă majoră de conflict.

O amenințare majoră la adresa securității națiunilor este reprezentată și de *modificările climatice*, în sensul accentuării procesului general de încălzire, cauzată de emisiile de gaze care amplifică *efectul de seră*. Una din consecințele

[105] Prof dr. Viorel Roman, *Religiile — surse de conflict*, în *"Situația statelor într-o lume în curs de mondializare"*, Editura Academiei de Înalte Studii Militare, București, 1992, p. 82–83.

încălzirii este accentuarea procesului de topire a gheților și creșterea nivelului mărilor.

Un factor de risc la adresa securității naționale îl constituie *acțiunile care afectează securitatea sistemelor informatice* din diverse locuri de concentrare a datelor cu caracter secret de stat sau confidențial de interes național. În acest sens, pot fi amintite: accesul neautorizat al unor grupuri de interese străine la bazele de date din calculatoarele diverselor instituții, decriptarea acestora și analizarea traficului de mesaje; penetrarea băncilor de date informatizate, inclusiv prin racolarea operatorilor ce lucrează în astfel de sisteme; accesarea sistemelor informatice care vizează derularea unor operațiuni comerciale ori financiar-bancare; inducerea unor disfuncții serioase în rețelele de calculatoare ale instituțiilor publice, inclusiv prin realizarea și difuzarea unor „viruși informatici" etc.

La acestea se adaugă luarea unor măsuri insuficiente de protecție contrainformativă la diverse niveluri decizionale; neajunsurile în pregătirea contrainformativă a unor factori de decizie; carențele organizatorice și de înzestrare umană și materială a instituțiilor statului care au atribuții în domeniul siguranței naționale; lipsa de reacție eficientă a factoriilor de decizie în urma informărilor, sesizărilor și atenționărilor realizate de serviciile de informații în legătură cu pericolele, riscurile și amenințările la adresa securității naționale etc.

Nesesizarea complexității și multitudinii factorilor de risc de natură externă la adresa securității naționale conduce la strategii simpliste de securitate, limitate la efecte evidente și imediate, dar niciodată adecvate unei securități durabile, construită prin acțiuni conjugate de tip preventiv în planuri multiple.

RISCURI DE NATURĂ INTERNĂ LA ADRESA SECURITĂȚII NAȚIONALE

Schimbările de natură politică, economică și socială care au avut loc pe scena internațională, în principal sud-est europeană, după 1989, au fost însoțite de amplificarea și diversificarea factorilor de risc intern la adresa securității și siguranței naționale. Ca rezultat al acestor tranformări, România, alături de celelalte țări din ziâonă, a trebuit să se adapteze noului mediu de securitate radical schimbat, să elaboreze și să implementeze politici și strategii de securitate care să corespundă noului context de securitate. Mai mult, evenimentele de la 11 septembrie 2001 au determinat o nouă redefinire a contextului de securitate și implicit a priorităților privind politica de securitate și siguranță națională, pentru a include terorismul și proliferarea armelor de distrugere în masă ca amenințări globale ce necesită a abordare conjugată a întregii comunități internaționale.

Astfel, la nivel intern, *Strategia de Securitate Națională a României*, adoptată la 18 decembrie 2001 prevede că obiectivele majore ale politicii privind siguranța națională au în vedere prevenirea și combaterea fenomenului infracțional, protejarea cetățenilor, a proprietății private și a celei publice și a infrastructurii de interes strategic. De asemenea, sunt enumerate principalele direcții de acțiune în domeniul siguranței naționale și a ordinii publice, combaterea terorismului, corupției și crimei organizate fiind considerate un obiectiv major al acestei strategii.

Potrivit *Strategiei de securitate a națională a României*, se consideră că principalele riscuri la adresa securității naționale sunt „nemilitare, în special de natură internă", fiind menționate aici riscurile de natură economică, financiară, socială și de mediu. Admițând că, la nivel intern, situația actuală de securitate a României este „caracterizată de numeroase vulnerabilități în aproape toate sferele mediului

economic și social", ca rezultat direct al presiunilor cumulative exercitate, de-a lungul timpului, de o multitudine de factori — politici, economici, financiari, sociali, culturali, biologici, religioși, demografici, militari sau de altă natură —, Strategia se securitate națională propune o evaluare adecvată a acestor vulnerabilități, astfel încât „răspunsurile și reacțiile sistemului național de securitate să fie în concordanță cu realitatea și, în același timp, permanent subordonate intereselor fundamentale ale țării".

Același document subliniază că „principalele probleme de securitate ale României sunt cele de ***natură economică"***, menționându-se aici: *menținerea problemelor economice, financiare și sociale generate de tranziția prelungită și de întârzierea finalizării reformelor structurale; nivelul crescut de corupție și managementul defectuos al resurselor publice, care pot duce la adâncirea inegalităților sociale și la proliferarea economiei subterane; răspunsul ineficient al instituțiilor statutului la probleme precum criminalitatea economică și tulburarea ordinii publice și siguranței cetățenilor, ceea ce poate genera scăderea coeziunii și solidarității sociale și a standardelor de viață ale cetățenilor; menținerea unor surse potențiale de conflict care pot duce la încetinirea sau stoparea proceselor și activităților economice curente, ca și starea de spirit a populației.*

Fără a fi explicit menționate în Strategia de securitate națională, la acestea riscuri de natură economică pot fi adăugate: pierderea controlului statului asupra unor sectoare, domenii sau obiective economice strategice, precum și pierderea unor importante piețe externe și interne de desfacere pentru produsele și serviciile românești; activitățile ilicite caracteristice economiei subterane susținute cu procedee proprii crimei organizate; spionajul economic în dauna României; coruptibilitatea unor persoane care, prin nivelul și natura funcției în societate pot avea, prin acțiunea sau

inacțiunea lor, o influență profund negativă în gestionarea resurselor naționale; blocarea sau perturbarea gravă a infrastructurii esențiale pentru economia națională (sistemul energetic, de transport și telecomunicații, financiar-valutar ș.a.); falimentarea unor sectoare economice strategice, etc.

Strâns legate de riscurile de natură economică, sursele de insecuritate de *natură socială*, manifestate în principal prin agravarea stării de sărăcie a unei mari părți a populației, menținerea și adâncirea decalajelor sociale între cetățenii țării, discriminările de orice natură, blocarea accesului unei părți a populației la serviciile sociale de bază etc., pot avea efecte dramatice în planul stabilității interne.

În *domeniul politic*, cum democrația și statul de drept sunt considerate *„resurse importante ale mediului intern de securitate"*, prezervarea acestor caracteristici, a stabilității politice, a pluralismului politic și a respectului pentru drepturile omului și cetățeanului sunt vitale pentru asigurarea securității naționale. În acest sens, *scăderea încrederii cetățenilor în instituțiile statului ca rezultat al indolenței și birocrației excesive a aparatului administrativ* este văzută ca un important factor de risc la adresa securității naționale, alături de *incapacitatea acestor instituții de a lua măsuri eficiente pentru dezvoltarea echitabilă a tuturor regiunilor țării și pentru îndeplinirea angajamentelor asumate în vederea integrării în structurile euro-atlantice de securitate.*

În domeniul *ordinii publice și siguranței naționale,* sursele de insecuritate sunt multiple și complexe, dintre acestea putând fi enumerate: crima organizată, traficul ilegal de droguri, de arme și muniții, de persoane etc., și, în general, criminalitatea transfrontalieră, indiferent de forma de manifestare; existența unor tensiuni sociale grave din diverse cauze (politicie, economice, etnice, religioase etc.); confruntările între diferite grupuri sociale, actele de violență

produse în cadrul unor adunări sau manifestări publice care pot degenera în revolte de mare amploare ce pun în pericol statul de drept.

În domeniul *siguranței naționale*, posibile surse de insecuritate pot fi: spionajul împotriva României; racolarea sau influențarea de către servicii străine de informații a unor demnitari români sau persoane care pot aduce prejudicii grave intereselor naționale fundamentale; penetrarea de către unele servicii de spionaj străine a structurilor ce compun sistemul național de apărare ori a structurilor în cadrul cărora se elaborează decizii sau propuneri importante pentru evoluțiile economice, social-politice, de apărare, ordine publică, de siguranță națională etc. ale României; acțiunile unor cercuri externe sau interne pentru tensionarea climatului de conviețuire a comunităților etnice cu populația majoritară, promovarea în plan extern sau intern a unor idei și imagini negative asupra României.

În *domeniul juridic*, sursele se insecuritate se pot manifesta prinî cadrul normativ prea permisiv sau excesiv de strict; corupția și traficul de influență în cazurile soluționării juridice a diferitelor cauze; hotărâri și soluționări judecătorești în contradicție flagrantă cu spiritul și textul legii, precum și cu realitatea ș.a..

Strategia de securitate națională face referire expresă la nerespectarea regulilor de protecție a informațiilor clasificate, acțiunile care afectează securitatea sistemelor informaționale din diverse locuri de concentrare a datelor cu caracter secret de stat sau confidențial de interes național putând fi sintetizate după cum urmeazăî accesul neautorizat al unor grupuri de interese străine la bazele de date din calculatoarele diverselor instituții, decriptarea acestora și analizarea traficului de mesaje; penetrarea băncilor de date informatizate, inclusiv prin racolarea operatorilor ce lucrează în astfel de sisteme; accesarea sistemelor informatice care

vizează derularea unor operațiuni comerciale ori financiar-bancare, etc. La acestea se pot adăuga: luarea unor măsuri insuficiente de protecție contrainformativă la diverse niveluri decizionale; neajunsurile în pregătirea contrainformativă a unor factori de decizie; carențele organizatorice și de înzestrare umană și materială a instituțiilor statului care au atribuții în domeniul siguranței naționale; lipsa de reacție eficientă a factoriilor de decizie în urma informărilor, sesizărilor și atenționărilor realizate de serviciile de informații în legătură cu pericolele, riscurile și amenințările la adresa securității naționale etc.

În *domeniul sanitar*, sursele de insecuritate sunt numeroase, fiind generate și alimentate în principal de condițiile socio-economice precare ale unei mari părți a populației țării (nivel scăzut de trai, condiții grele de muncă, stres, alimentație proastă). Astfel, diverse boli și epidemii precum tuberculoza, HIV/SIDA, bolile cardiovasculare etc., sunt destul de răspândite în România, numărul bolnavilor crescând continuu. De asemenea, consumul excesiv de alcool, țigări și, în ultimii ani, de droguri, manifestat mai ales în rândul tinerilor, reprezintă un pericol real la adresa securității interne. Dacă până acum câțiva ani România era doar de tranzit pentru drogurile traficate ilegal din Asia și Africa spre Europa Occidentală, acum țara noastră prezintă și caracteristicile unei țări consumatoare.

În ceea ce privește *domeniul demografic*, în România, procesul de îmbătrânire demografică continuă să progreseze, cauza principală fiind scăderea pe termen lung a natalității și creșterea ratei mortalității, ceea ce determină schimbarea structurii pe vârste a populației, respectiv creșterea ponderii bătrânilor și scăderea ponderii tinerilor. Dacă în urmă cu 50 de ani ponderea bătrânilor (considerați de la 60 de ani în sus) era de 7% în populația totală, azi această pondere depășește 18%, în timp ce populația tânără reprezintă mai

puțin de 20%, față de o treime din populație, cât era în urmă cu câteva decenii.

Tot în domeniul demografic un important factor de risc este și *migrația populației, în principal a tinerilor și specialiștilor din diverse sfere de activitate*, fenomen care nu numai că duce la scăderea populației și modificarea structurii acesteia, dar afectează și *potențialul de dezvoltare a societății românești.*

Strategia de securitate națională mai menționează, ca surse interne de insecuritate, *nerespectarea normelor de mediu în funcționarea unor întreprineri industriale*, ceea ce poate duce la generarea unor dezastre ecologice, catastrofe naturale și degradarea mediului. Astfel, se impune cu necesitate reevaluarea politicii de protecție a mediului din perspectiva vulnerabilității unor zone cu risc ecologic.

În domeniul tehnologic, este amintită *menținerea unui nivel scăzut al tehnologiei informaționale și blocarea dezvoltării acesteia la standardele cerute de dinamica globalizării.*

La toate aceste surse de insecuritate se mai pot adăuga și altele, spre exemplu cele din *domeniul culturii și educației*, manifestate prin lipsa de respect față de valorile culturale tradiționale și promovarea unor subculturi precum și a unor valori contrare intereselor naționale, lipsa unui sistem educațional adaptat cerințelor societății contemporane etc.

MĂSURI DE CONTRACARARE A FACTORILOR DE RISC ȘI AMENINȚARE LA ADRESA SECURITĂȚII NAȚIONALE A ROMÂNIEI ÎN PRIMUL DECENIU AL SECOLULUI XXI

În contextul transformării mediului internațional de securitate, în primul rând prin apariția și multiplicarea noilor tipuri de riscuri și amenințări, România a acordat o

atenție sporită asigurării securității naționale prin identificarea și dezvoltarea unor mijloace și instrumente coerente de combatere și contracarare a acestora. În acest sens, se au în vedere două dimensiuni majore: pe de o parte, intensificarea cooperării la nivel intern între instituțiile cu atribuțiuni în domeniu, precum și dezvoltarea unor căi de acțiune specifice, iar, pe de altă parte, cooperarea permanentă cu structurile și instituțiile internaționale specializate în sensul eficientizării eforturilor de combatere a unui spectru larg de riscuri și amenințări.

Există o strânsă conexiune între cele două dimensiuni, internă și externă, iar o strategie coerentă pentru contracararea amenințărilor la adresa securității depinde de buna funcționare a acesteia. Inițierea și coordonarea acțiunilor naționale în domeniul securității se bazează pe un ansamblu de legi și documente fundamentale care formulează, în mod clar, principalele căi și mijloace de acțiune în acest domeniu: Constituția României, Strategia de Securitate Națională, Strategia Militară, Carta Albă a Securității și Apărării Naționale etc. Sistemul legislativ românesc este racordat la imperativul apărării intereselor naționale și la asigurarea securității în toate dimensiunile sale. Noile riscuri apărute la adresa securității și a valorilor societății românești determină schimbări în structura și modul de funcționare a principalelor instituții cu atribuțiuni în domeniu (Ministerul Apărării, Minsiterul de Interne, Ministerul de Justiție, Serviciul Român de Informații, Serviciul de Informații Externe) care trebuie să fie capabile să răspundă noilor provocări și amenințări.

Ca răspuns la amenințările la adresa securității naționale este necesară folosirea unitară și coerentă a tuturor capacităților pentru îndeplinirea obiectivelor naționale de securitate. Modalitățile de acțiune pentru asigurarea securității naționale sunt stabilite în funcție de interesele țării,

de resurse, de evoluția proceselor economice și politico-militare, precum și de potențialii factori de risc. România a inițiat o serie de măsuri și acțiuni specifice, de combatere a diferitelor tipuri de riscuri și amenințări, în special în domeniile: politica externă, economico-financiar, social, siguranța națională, ordine publică și apărare națională.

În domeniul politicii externe, pot fi identificate o serie de modalități de acțiune și căi de diminuare a vulnerabilităților și creșterii gradului de securitate națională:

- participarea responsabilă la activitățile și procesele decizionale ale Alianței Nord-Atlantice precum și la misiunile internaționale sub egida NATO, având ca scop combaterea terorismului și proliferarea armelor de distrugere în masă;
- dezvoltarea de relații privilegiate cu țările UE, precum și a Parteneriatului Strategic cu SUA;
- participarea României la procesul de realizare a Identității Europene de Securitate și Apărare;
- susținerea dimensiunii pan-europene a OSCE, ca forum de dialog în domeniul securității și dezvoltarea capacității de acțiune pentru prevenirea conflictelor, gestionarea crizelor și reconstrucția post-conflict;
- susținerea diplomatică a participării la operațiunile de pace ale ONU și la alte acțiuni vizând asigurarea stabilității și întărirea încrederii la nivel regional și global;
- respectarea strictă a angajamentelor internaționale în domeniul neproliferării și controlului armamentelor, exporturilor de produse strategice și de tehnologie cu dublă utilizare, precum și participarea activă la dezbaterile, din diverse foruri, pe această temă;
- promovarea unei politici active în plan bilateral sau într-un cadru internațional pentru asigurarea securității și stabilității în Europa de Sud-Est, ca și în Caucazul de Sud și întreaga regiune a Dunării și Mării Negre;

• dezvoltarea unor parteneriate bi- și trilaterale cu statele din regiune, inițierea și participarea la proiecte de cooperare subregională, transfrontalieră și în cadrul euroregiunilor.

Relansarea economică trebuie consolidată prin crearea unui mediu de afaceri atractiv și stabil și prin racordarea adecvată la marile fluxuri economico-finaciare, tehnologice și comerciale. Accelerarea creșterii economice vizează în primul rând asigurarea prosperității cetățenilor și sprijinirea procesului democratic intern. În domeniul economico-financiar, principalele modalități de acțiune pentru asigurarea securității naționale, prin diminuarea vulnerabilităților și reducerea riscurilor și amenințărilor inerente perioadei de tranziție, sunt următoarele:

• asigurarea stabilității funcționale a economiei naționale;

• asigurarea resurselor financiare pentru consolidarea sistemelor de apărare, ordine publică și siguranță națională;

• realizarea unui sistem economico-financiar modern fundamentat pe o economie de piață, construită pe baza principiilor eficienței, justiției și solidarității sociale;

• susținerea inițiativei private prin perfecționarea cadrului economico-financiar, legislativ și instituțional;

• accelerarea procesului de armonizare legislativă în domeniul financiar și de implementare a standardelor europene;

• corelarea politicilor economice naționale cu procesul realizării uniunii economice și monetare europene;

• dezvoltarea capacităților de cercetare și producție în domeniul militar;

• realizarea măsurilor pentru stabilizarea macroeconomică, accelerarea reformelor structurale în economie, lărgirea și consolidarea sectorului privat, atragerea investițiilor străine și sprijinirea întreprinderilor mici și mijlocii;

• armonizarea legislației economico-financiare și a politicilor fiscale cu legislației europeană și cerințele normelor

și directivelor Uniunii Europene, în perspectiva aderării României la acest organism;

• conectarea României la marile axe și transport continentale și transcontinentale și cearea infrstructuriloe informaționale;

• dezvoltarea cooperării economice internaționale, prin forme noi, mai active și stimulative de comerț exterior.

În ceea ce privește domeniul social, se pune accent pe realizarea unor modalități de stimulare a solidarității naționale și a responsabilității civice. Acțiunile promovate în acest domeniu au în vedere:

• promovarea dialogului și coeziunii sociale prin implicarea statului, ca factor de echilibru, în contracararea efectelor negative ale procesului de tranziție și evoluțiilor economiei de piață;

• reforma sistemului de securitate socială și diminuarea deficitului de finanțare a protecției sociale;

• descentralizarea deciziei administrative în domeniul raporturilor de muncă;

• ocuparea forței de muncă în concordanță cu orientările UE, diminuarea șomajului și asigurarea unei protecții sociale reale a șomerilor, inclusiv prin atragerea și implicarea acestora în activități de utilitate publică, desfășurate în perioada disponibilizării;

• instituirea unei politici salariale corespunzătoare performanțelor și importanței domeniului;

• perfecționarea sistemului de asistență socială;

• dezvoltarea civismului, a solidaritățăii sociale și a dialogului intercultural.

În domeniul siguranței naționale și ordinii publice, prin măsurile adoptate, se are în vedere asigurarea capacității analitice și operaționale a serviciilor de informații. Acestea vor acționa pentru anticiparea amenințărilor la adresa securității naționale, astfel, încât, împreună cu celelalte insti-

tuții ale statului, să contribuie la apărarea și promovarea intereselor naționale ale țării. Acțiunile specifice în domeniul menținerii ordinii publice vizează, cu prioritate, prevenirea și combaterea fenomenului infracțional, protejarea cetățenilor, a proprietății private și publice. Principalele modalități în acest sens sunt:

• asigurarea controlului civil asupra instituțiilor din domeniul siguranței naționale și ordinii publice;

• dezvoltarea și perfecționarea modalităților de cunoaștere și contracarare a riscurilor și amenințărilor la adresa securității naționale, evaluarea complexă a dinamicii acestora;

• informarea promtă și corectă a factorilor de decizie ai statului, instituirea unui sistem eficient de gestionare, valorificare și protejare a informațiilor secrete în condițiile respectării dreptului la informare a cetățenilor;

• instituționalizarea unor forme de cooperare permanentă între structurile care contribuie la realizarea siguranței naționale și ordinii public;

• consolidarea lanțului instituțional de acțiune (Poliție, Servicii de Informații, Minister Public, Justiție) și intensificarea activităților desfășurate de acestea împotriva corupției și crimei organizate;

• cooperarea internațională în domeniul combaterii criminalității transnaționale;

• sporirea securității frontaliere prin cooperarea poliției de frontieră cu organele vamale, precum și utilizarea unei evidențe computerizate și a supravegherii prin satelit;

• consolidarea relațiilor de parteneriat între serviciile de informații din România și cele din statele membre ale NATO și UE;

• cooperarea cu serviciile de informații ale altor state, în cadrul relațiilor bi- și multilaterale ale României, în scopul sporirii securității proprii și a celei internaționale.

În ceea ce privește domeniul apărării naționale, armata română se află într-un proces de redefinire, redimensionare și restructurare care are ca scop final crearea unei armate de dimensiuni mici, mobile, capabilă să desfășoare o gamă largă de misiuni. Ca membru NATO, România va trebui să dispună de o armată modernă și bine instruită, care să poată desfășura, alături de ceilalți aliați, acțiuni vizând reglementarea diferendelor internaționale, prevenirea conflictelor, gestionarea crizelor și apărarea colectivă. Principalele măsuri vizate, în domeniul apărării naționale, în ceea ce privește combaterea riscurilor și amenințărilor, sunt:

• întărirea capacității de descurajare, prin realizarea și menținerea unei forțe militare moderne și credibile, dotată cu tehnică și echipament militar modern și deservită de personal profesionalizat, cu o pregătire adecvată;

• constituirea în cadrul forțelor armate a instrumentelor operaționale moderne, capabile să permită României să ia parte activ, ca membru cu drepturi depline, la eforturile Alianței Nord-Atlantice și ale organismelor internaționale care vizează reglementarea diferendelor internaționale, prevenirea conflictelor, gestionarea crizelor și apărarea colectivă, precum și participarea la operațiunui militare multinaționale în sprijinul păcii, la întărirea încrederii și stabilității în Europa Centrală și de Sud-Est, la acțiuni cu caracter umanitar și alte activități militare;

• constituirea și consolidarea capacităților necesare pentru îndeplinirea performantă a obligațiilor asumate de România, de a participa în cadrul unor operațiuni de menținere a păcii, de salvare, de răspuns la crize, de combatere a terorismului și de asistență umanitară, la nivel subregional și regional;

• accelerarea realizării programelor prioritare de interoperabilitate cu structurile militare ale Alianței Nord-Atlantice îndeosebi în domeniile pregătirii personalului, instruirii

trupelor, sistemelor C4I (comandă, control, comunicații, computere, informații), managementuluui și apărării spațiului aerian, logistic și infrastructurii;

• menținerea la un nivel corespunzător a unei capacități de intervenție în caz de urgență civilă;

• îmbunătățirea colaborării între serviciile de specialitate, pe linia schimbului operativ de informații, vizând potențialii factori de risc la adresa securității și stabilității interne.

Agravarea amenințării teroriste, mai ales după 11 septembrie 2001, și declanșarea campaniei internaționale de luptă împotriva terorismului și armelor de distrugere în masă, au impus, cu necesitate, crearea unor mecanisme și a unor structuri naționale cu atribuțiuni specifice în acest sens. Pe 5 aprilie 2002, a fost adoptată Strategia națională de prevenire și combatere a terorismului care își propune ca obiective majore:

• identificarea, monitorizarea și evaluarea constantă a tuturor riscurilor și amenințărilor respectiv a vulnerabilităților la adresa securității naționale care pot contribui la apariția și dezvoltarea terorismului;

• protejarea teroritoriului național, al populației și a obiectivelor românești din interior și exterior de activitățile asociate terorismului;

• prevenirea implicării cetățenilor români și rezidenților străini din România în activități subsumate terorismului internațional;

• participarea la eforturile internaționale de prevenire și combatere a fenomenului terorist, prin:

– contribuții active la inițiativele bi-și multilaterale, acțiuni politico-diplomatice, reglementări și instrumente normative, mecanisme interna-ționale de cooperare interinstituțională menite să prevină apariția, dezvoltarea și manifestarea fenomenului terorist;

– transpunerea în cadru normativ a obligațiilor asumate de statul român;

– schimb de informații și participarea cu forțe armate specializate la operațiuni militare multinaționale sub mandat ONU, destinate prevenirii și combaterii terorismului.

În vederea implementării obiectivelor din strategie, a fost constituit Sistemul național de prevenire și combatere a terorismului, coordonat, la nivel strategic, de CSAT, iar, la nivel tehnic/operațional, de către SRI. La nivelul SRI a fost constituit Centrul de Coordonare Operativă Antiteroristă.

Principalele misiuni pentru prevenirea terorismului sunt: activități informativ-operative, derulate în interiorul și exteriorul teritoriului național; activități împotriva fluxurilor de alimentare cu resurse umane, financiare, logistice și informaționale a organizațiilor teroriste; activități de pază, protecție și alte forme speciale de descurajare pentru asigurarea securității principalelor categorii de factori umani și de obiective autohtone și străine de pe teritoriul național, precum și a principalelor obiective românești din străinătate, potențial vizate de acțiuuni teroriste; activități de pregătire a intervenției în urgențe civile generate de acțiuni teroriste cu diverse mijloace specifice, în vederea limitării/combaterii efectelor acestora; activități destinate optimizării continue a cadrului legislativ privind acțiunile teroriste.

Misiunile privind combaterea terorismului se realizează prin: activități de sancționare preliminară sau, după caz, post factum, a preocupărilor și faptelor subsumate terorismului; intervenția antiteroristă nemijlocită, în cazurile în care sunt iminente, se derulează ori au avut loc acțiuni teroriste; participarea la operațiuni de prevenire și combatere, prin cooperare internațională, a terorismului pe diverse spații.

II. FENOMENUL CORUPȚIEI ȘI IMPACTUL ASUPRA SECURITĂȚII ȘI SIGURANȚEI NAȚIONALE

CORUPȚIA, O PROBLEMĂ LA NIVEL NAȚIONAL

Dr. William Brânză

„Nimic nu e mai periculos pentru conștiința unui popor decât privelișteа corupției"

M. Eminescu

Aflându-se într-o perioadă de tranziție, statul român, se confruntă cu problema corupției, a cărei apariție a fost favorizată de criza instituționalizată în special la nivel local, constatându-se o scădere a mijloacelor de investigație, a controlului social și normativ, o criza de autoritate și de credibilitate a unor instituții, o slabă influență a normelor legale asupra comportamentului indivizilor, o implicare a unor persoane cu răspundere și a unor funcționari publici în mari afaceri ilegale și abuzuri. O altă cauză a corupției o constituie atât descentralizarea deciziilor și a structurilor administrative, autonomia funcțională, lipsa de fermitate a unor organe de control specializate, cât și lipsa unei legislații corespunzătoare, care au încurajat criminalitatea și au amplificat corupția. Starea de criză a tranziției societății românești a dus la scăderea nivelului de trai, la accentuarea și generalizarea sărăciei, fapte ce determină uneori o anumită îngăduință față de corupție[106].

[106] Viorel Stranciug, Gheorghe Hurjui, *Considerații generale privind fenomenul corupției. Preocupări, măsuri și sugestii pentru perfecționarea structurilor și mijloacelor de ripostă împotriva acestui flagel*, în „Revista de criminologie și criminalistică", nr. 1/1999, p. 50.

Reprezentând un fenomen social complex, cu modalități de manifestare și consecințe sociale ce interesează atât populația cât și factorii de control social, corupția este percepută ca o problemă de o amploare deosebită, ce subminează structurile de putere și de autoritate[107]. Corupția afectează întreaga societate, ea adaptându-se rapid și eficient la ritmul schimbărilor petrecute în spațiul românesc.

Corupția este prezentată în majoritatea sectoarelor cheie ale vieții sociale, politice și economice[108], vizând:

– *domeniul financiar bancar*, unde comiterea faptelor de corupție este încurajată de mai mulți factori, cum ar fi: acordarea sau facilitarea obținerii preferențiale a unor credite de către diverși funcționari bancari, emiterea de documente de plată ale unor instituții de credit fără existența garanției sau a acoperirii necesare efectuării anumitor operațiuni, acordarea de credite cu dobândă bonificată în baza unor documente false;

– *domeniul economic*, unde infracțiunile de corupție săvârșite au legătură cu procesul de privatizare, de evaluare și de vânzare a activelor societăților cu capital de stat, cu transferurile ilegale de capital și de patrimoniu, cu implicarea în activitățile cu caracter privat a unor persoane din conducerea unor unități de stat;

– *sectorul metalurgic*, al construcțiilor de mașini, siderurgic și energetic, evident dezavantajate prin încheierea unor contracte generatoare de prejudicii pentru unitățile cu capital de stat. Astfel, au fost încheiate tranzacții cu firme, care nu prezentau garanție și care nu și-au respectat obligațiile contractuale în detrimentul statului român, dar în avantajul unor persoane cu funcții de conducere în cadrul instituțiilor cu atribuții în privatizarea societăților cu capital de stat;

– *domeniul petrolier*, unde infracțiunile de corupție s-au comis în legătură cu aprovizionarea, transportul, prelucrarea

---

[107] V. Dobrinoiu, *op. cit.*, p. 34.

[108] *Serviciul Anticorupție din cadrul Direcției de Combatere a Criminalității Economico-Financiare I.G.P*, București, 2002.

și valorificarea țițeiului și a produselor derivate, în scopul obținerii de avantaje materiale personale, lucru realizat în sprijinul unor persoane cu influență în luarea deciziilor din sistemul administrației de stat. Astfel, statul roman a fost prejudiciat prin exportarea de produse petroliere la prețuri mai mici decât cele interne și sub prețul bursei internaționale;

– *domeniul flotei marine*, fluviale și de pescuit oceanic, unde s-au comis numeroase ilegalități care au determinat intervenția staului român. Astfel au fost închiriate nave unor firme constituie ad-hoc, generând în sarcina marilor proprietari obligații financiare ce au fost acoperite de stat;

– *domeniul administrației publice*, unde fenomenul corupției este la ordinea zilei, devenind o obișnuință la nivelul acordării de autorizații pentru întreprinzătorii privați, repartizări de terenuri pentru construcții, de locuințe și spații pentru firme particulare, la nivelul trimiterii de forță de muncă în străinătate;

– *serviciile publice*, în cadrul cărora actele de corupție se comit pentru legalizarea de acte fictive, pentru înregistrarea de mențiuni ce nu corespund realității în Registrul Comerțului în vederea obținerii autorizației de funcționare de către societatea comercială, legalizarea de documente privind scutirea de impozite sau stabilirea acestora sub nivelul veniturilor realizate, acordarea de vize în mod ilegal. Cele mai vulnerabile instituții în acest domeniu, par a fi organele de control financiar, funcționarii și demnitarii din departamentele ministeriale, oficiile pentru protecția consumatorilor, Garda Financiară, agenții fiscali, funcționarii din sistemul bancar, din industrie, din primării și din prefecturi, personalul unităților vamale, Registrul Comerțului;

– *ramurile productive*, unde fenomenul corupției se resimte la nivelul aprovizionării, al transferurilor ilegale de patrimoniu, prin subevaluări de la societățile naționale la întreprinzătorii privați;

– *domeniul comerțului și al prestărilor de servicii*, caracterizat prin vânzarea de produse necorespunzătoare calitativ, condiționarea executării unor prestații de servicii la

prețuri depășind tarifele legale și pretinderea de avantaje pecuniare pentru lucrările comandate, condiționarea emiterii licențelor de import-export. Probleme există în ultimul timp în domeniul dreptulurilor de autor, al drepturilor conexe și al copyright-ului, în domeniul repartizării locuințelor din fondul locativ de stat, în privința declarării sau schimbării sediilor sociale ale societăților comerciale;

– *în sectorul instituțiilor bugetare din sănătate și din învățământ*, situația nu diferă prea mult în comparație cu celelalte domenii. În domeniul sănătății, corupția este larg răspândită, mita sub forma „micilor atenții", fiind oferită de doi dintre subiecții chestionați. Fenomenul este frecvent și în legătură cu promovarea unor examene și eliberarea de certificate medicale, de acte constatatoare medico-legale, în legătură cu intervenții chirurgicale, cu ședere prelungită în spitale și cu distribuirea de medicamente.

Pentru ca reforma în această direcție să aibă rezultate pozitive, este recomandat ca în locul practicării unui sistem de plăți neoficiale să se realizeze o îmbunătățire a managementului și o redresare a deficiențelor financiare în sectorul sanitar. Trebuie, de asemenea, înțeles, faptul că serviciile gratuite nu pot persista într-un mediu bazat pe bugete sărace, limitarea întinderii acestora și introducerea taxelor conferind o notă de realism sistemului[109]. Cel mai grav prejudiciu cauzat de corupție în sistemul sanitar este efectul pe care corupția îl are asupra deciziilor de a asigura sau nu tratament. În cazul familiilor sărace există o probabilitate de două ori mai mare de a afirma că nu au apelat la asistența medicală chiar dacă ar fi fost nevoie. În acest mediu există concepția că fenomenul corupției este larg răspândit în sistemul sanitar[110].

În învățământ, mai mult de jumătate dintre persoanele chestionate au declarat că au efectuat plăți neoficiale cadre-

[109] Mauren Lewis, *Who is Paying for Health Care in Easteern Europe and Central Asia?* World Bank 2000 Washington D.C.

[110] *Studii privind corupția în România*, World Bank, 2000.

lor didactice, dar nu la cererea acestora din urmă, ci din inițiativă proprie, aceste plăți fiind manifestări de recunoștință. Sistemul de învățământ este perceput ca fiind o instituție coruptă pe scară largă.

Unul dintre domeniile cele mai corupte în România îl constituie *sistemul judiciar*. Mita este oferită aici atât pentru accelerarea sau tergiversarea desfășurării procesului, fără a exista motive întemeiate, ori pentru ca judecata unei cauze să revină unei anumite persoane, cât și pentru schimbarea unor hotărâri judecătorești în favoarea corupătorilor.

Poliția este o altă instituție susceptibilă de a fi atacată de corupție. Majoritatea persoanelor chestionate a afirmat că nu are încredere în sistemele de investigare ale poliției și în rezultatele acestora, pe când nivelul plăților neoficiale practicate la acest nivel este relativ scăzut: de 3–7%.

Corupția, în funcție de domeniile pe care le atacă, poate îmbrăca mai multe forme: economică (gestiunea frauduloasă, abuzul de putere, înșelăciunea, bancruta frauduloasă, escrocheria, contrafacerea mărfurilor și produselor, falsuri în evidențele bancare și contabile); profesională care cuprinde luarea și darea de mită, traficul de influență, abuzul în serviciu; politică.

Pentru a putea ajunge la o reală dimensionare a fenomenului corupției și a cauzelor acestuia, e necesară o abordare interdisciplinară ținând cont de elementele care îl garantează, indiferent de natura acestora.

Dintre condițiile ce au favorizat multiplicarea fenomenului corupției, cele mai importante sunt: deficiența procesului de privatizare, a modului de concepere și de aplicare a reformei, perpetuarea și consolidarea vechii birocrații, blocaje și inadvertențele apărute în cadrul descentralizării politico-administrative și nu în ultimul rând, sărăcia.

Dintre cauzele corupției, cea mai importantă pare a fi legislația deficitară.

În orice sistem, eficiența și valabilitatea legislației, concretizate în forța ei obligatorie, include gradul de credibilitate și de legitimitate al acesteia și eficiența regulii de drept în

raport de obiectivele urmărite. Normele juridice adoptate de-a lungul anilor, au neglijat condițiile de tehnica legislativă , dar și modificările suferite de diversele domenii avute în vedere.

De multe ori, legea nu este expresia voinței cetățenilor, ea fiind rezultatul unor interese de grup, conjuncturale. Astfel, în momentul de față, statul roman se confruntă cu sisteme ineficiente de legi, cu inflație legislativă. Conform studiului realizat de Banca Mondială în România, în cursul anului 2000, legislația deficitară a fost invocată de întreprinderi și de funcționarii publici, ca fiind o cauză majoră a corupției.

Reglementările excesive și instabile se află pe locul al treilea în topul factorilor ce au avut un rol negativ asupra activității firmelor, secondând inflația și devalorizarea monetară. Un studiu efectuat în 1999 de centru IRIS asupra firmelor, confirmă obstacole legislative cu care se confruntă acestea. Unei firme tipice i se cer să obțină între 23 și 29 de aprobări autorizări și licențe provenind de la diverse instituții, ce costă între 10 și 60 milioane de lei și a căror completare durează de la 49 la 102 zile. Un alt obstacol îl constituie inspecțiile efectuate firmelor care pierd între 14 și 38 de zile cu pregătirea actelor și așteaptă apoi încă două sau trei săptămâni după terminarea inspecției pentru aprobările oficiale[111].

Cauze de ordin politic includ comportamentele care deviază de la exercitarea îndatoririlor normale ale unui rol public. Drept exemplu în acest sens, putem aminti fapte privind economia națională, sistemul financiar bancar.

Cauze de natură administrativă sunt percepute ca având o importanță majoră în influențarea corupției.

Comportamentele coruptive sunt favorizate de o serie de factori ce țin de organizarea și conceptualizarea sistemului administrativ, cum ar fi inexistența unor regulamente de organizare și funcționare clare, neaplicarea criteriului competenței în selectarea și promovarea funcționarilor publici

——— [111] I.R.I.S — Analiza casetei roșii: Legislația și birocrația în România mai, 2000.

și perpetuarea practicilor ținând de relațiile extraprofesionale, salarizarea insuficientă a funcționarilor.

Nivelul salariului este de multe ori invocat în justificarea coruptibilității funcționarilor. Studiul efectuat de Banca Mondială, relevă faptul că, salariul este unul din multiplele elemente generatoare de corupție, dar el nu poate justifica creșterea fenomenului. Eforturile pentru îmbunătățirea realizărilor sectorului public include frecvent măsuri recompensatorii la adresa celor mai devotați funcționari. Un regim de recompensare a rezultatelor poate fi un bun stimulent, doar dacă este implementat de o manieră consecventă și transparentă. Cel mai frecvent motiv de corupție, invocat de 27% dintre cei chestionați, este reprezentat de calitățile personale ale salariaților, doar 17% dintre cei intervievați dând vina pe nivelul mic al salariilor și pe nerespectarea zilelor pentru efectuarea plăților. Nivelul corupției este mai scăzut în instituțiile care au proceduri avansate ale bugetului managerial, alături de reguli interne simple și clare, bine monitorizate. În ceea ce privește nivelul constrângerii din interiorul instituțiilor, 35% dintre cei intervievați s-au pronunțat pentru soluția nedepășirii lui în nici un mod. Corupția administrației afectează societatea în ansamblul său și ea trebuie redusă cât mai repede posibil.

Dintre cauzele de natură economică pot fi date ca exemplu reglementarea defectuoasă a unor activități economice (T.V.A, accize), subvenționarea anumitor categorii de produse sau servicii , acordarea de reeșalonări la plata obligațiilor față de stat fără garanții, promovarea unei economii de piață în condițiile unei penurii de capital, a unei economii subdezvoltate și a unei politici economice fără șanse.

Pe lângă aceste cauze, merită a fi puse în discuție și aspecte cu caracter etiologic corupției, privind mortalitatea societății, eficiența activității instituțiilor de influența morală, educațională și socio-culturală, într-un context în care societatea manifestă toleranță față de „mica corupție" și respect față de cei care au succese prin eludarea legii.

Înțelegerea efectelor corupției este necesară pentru a realiza cât de importantă este adoptarea unei strategii anticorupție la nivel național.

Corupția afectează siguranța națională, ceea ce duce la adâncirea inegalităților sociale și la profilarea economiei subterane. Acest aspect ține și de vulnerabilitatea situației interne a statului roman.

Pe plan socio-economic, efectele negative ale corupției sunt relevate în primul rând de creșterea ratei sărăciei. Creșterea economică și rata sărăciei sunt doi indicatori invers proporționali, așa încât, dacă statul se confruntă cu o perioadă de încetinire a creșterii economice, sunt limitate posibilitățile sale de dezvoltare. Corupția duce și la reducerea investițiilor străine directe, care au nevoie de existența unui climat de siguranță în mediile pe care vor să le câștige.

În România, familiile sărace resimt mai puternic efectele corupției, astfel acestea fac plăți neoficiale de două ori mai multe decât familiile cu venituri mai. Corupția generează creșterea ratei șomajului, încetinirea ritmului reformei.

În plan psihosocial, corupția reprezintă un stimulent pentru înmulțirea comportamentelor imorale, ea generează conflicte sociale, ca urmare a unui sentiment de frustrare a populației în fața corupției, determină încetinirea evoluției în procesul de tranziție.

Pe plan extern, corupția reprezintă un impediment evident în vederea aderării României la Uniunea Europeana și la alte organizații internaționale.

Înțelegând costurile sociale pe care le implică promovarea comportamentelor corupte într-o societate aflată în perioada de tranziție, este necesară aplicarea unor reforme imediate și a unor strategii care să vizeze combaterea fenomenului corupției.

CRIMINOGENEZA CORUPȚIEI

Dimitrie Bogdan Licu

Strategia de Securitate Națională inserează la loc de frunte între vulnerabilitățile de sorginte internă pe cele care se referă la accentuarea fenomenelor de corupție și de administrare deficitară a resurselor publice, ce produc adâncirea inechităților sociale și proliferarea economiei subterane. Dacă la acestea adăugăm reacțiile ineficiente ale instituțiilor statului în fața acutizării fenomenelor de criminalitate economică și de perturbare a ordinii publice și siguranței cetățeanului, avem imaginea dimensiunilor malefice ale corupției asupra ansamblului securității naționale.

Guvernul României are înscrisă printre prioritățile de guvernare, combaterea corupției prin măsuri radicale care să determine o reducere efectivă a ariei de manifestare a acestui flagel. Această voință politică clară, care susține necesitatea declanșării unei ofensive pe fondul prevenirii și combaterii corupției prin măsuri radicale, urmărește reducerea oportunităților de comitere a faptelor de această natură și oprirea evoluției fenomenului, prin care indivizi, grupuri de persoane, entități publice sau private ar putea influența, prin acte de corupție, procesele de elaborare și de adoptare a legislației, în scopul obținerii unor profituri ilicite.

În acest sens, prin H.G. nr.763 din 26 iulie 2001, s-a înființat Comitetul Național de Prevenire a Criminalității cu rol de elaborare, integrare, corelare și monitorizare a politicii Guvernului de prevenire a criminalității la nivelul național.

Grupul central de analiză și coordonare a activităților de prevenire a corupției, constituit în cadrul Comitetului, asigură implementarea și monitorizarea Programului Național de Prevenire a Corupției, precum și a Planului Național de Acțiune Împotriva Corupției, cuprinse în H.G. nr.1065 din 2 octombrie 2001.

Potrivit acestui act normativ au fost extinse preocupările instituțiilor și autorităților cu atribuții în limitarea fenomenului corupției, fără a afecta politica penală represivă în domeniu, prin derularea prioritară a unor acțiuni de prevenire, atacând baza corupției cu impact negativ pentru percepția publică.

Studiul de față are ca obiectiv analiza cadrului legislativ existent în domeniul prevenirii și combaterii fenomenului corupției în România.

Această analiză este cu atât mai necesară cu cât, în ultima perioadă, mai ales din anul 2000 până în prezent, cadrul normativ ce reglementează lupta împotriva corupției, a fost îmbogățit și completat, atât pentru armonizarea legislației interne cu cea internațională, cât și pentru a fi adaptat specificităților societății românești.

Istoria societății umane ne demonstrează că fenomenul infracțional al corupției a existat din cele mai vechi timpuri. Unii juriști consideră chiar că tendința omului spre corupție a existat din totdeauna.

Făcându-și apariția încă din antichitate, tot de pe atunci corupția este și reprimată, fiind aplicate și pedepse aspre și măsuri de prevenire și combatere, dar aceasta nu numai că a supraviețuit de-a lungul veacurilor, dar evident a și progresat. Corupția, ca fenomen social și ca delict infracțional, s-a dovedit a poseda o vitalitate de neinvidiat, dezvoltându-se o dată cu societatea, o dată cu statul și dreptul, căpătând noi forme de manifestări. Astăzi, problema corupției este plasată în centrul atenției opiniei publice din comunitatea europeană și din întreaga lume. Practic, zilnic, fie în presă, la radio sau televiziune, precum și în alte surse, se dau publicității diverse fapte de corupție în care sunt implicați reprezentanți ai autorităților puterii de stat, partidelor politice, funcționari de diverse ranguri aparținând unor organizații naționale, internaționale sau supranaționale.

Corupția constituie o amenințare pentru democrație, preeminența dreptului și drepturilor omului, subminează principiile de bună administrare, echitate și justiție socială,

denaturează concurența, împiedică dezvoltarea economică și pune în pericol stabilitatea instituțiilor democratice și bazele morale ale societății.

DEFINIȚIA ȘI FORMELE CORUPȚIEI

Printre definițiile clasice ale corupției întâlnim în mod curent: „abatere de la moralitate, de la cinste, de la datorie". Se remarcă, de asemenea, caracterul venal al corupției care, în fapt, înseamnă obținerea de foloase necuvenite prin orice mijloace și fără scrupul.

În codurile penale ale diferitelor state democratice există două mari accepțiuni ale conceptului:

a) pentru majoritatea sistemelor penale, ***corupția*** este „un concept prioritar normativ, desemnând încălcarea și transgresiunea ilegală și imorală a normelor referitoare la îndatoririle funcționarului public, agenților economici sau persoanelor care efectuează diferite operații financiare sau bancare";

b) în sens mai larg, pentru altele, ***corupția*** este definitivă ca „diferite acte sau fapte ilicite generate de utilizarea abuzivă sau frauduloasă a puterii, în scopul obținerii unor avantaje personale de către agenții publici, dar și fapte care privesc alte forme de obținere a unor foloase necuvenite".

Specialiștii dreptului penal, criminologiei și sociologiei criminalității apreciază că există trei forme importante ale fenomenului corupției.

Corupția profesională, care include marea majoritate a infracțiunilor de serviciu, comise în timpul serviciului de către funcționarii publici sau alte persoane din sectorul public, care încalcă normele deontologiei profesionale, prin îndeplinirea condiționată și preferențială a atribuțiilor lor legale.

Corupția economică, denumită și criminalitatea economico-financiară, ce include acte și fapte ilicite și ilegale comise

de indivizi, asociații, societăți sau organizații în legătură cu derularea unor afaceri și tranzacții financiar-bancare, vamale, comerciale, prin utilizarea înșelăciunii fraudei, abuzului de încredere, activității în urma cărora sunt prejudiciate interesele economice, colective sau particulare.

Corupția politică, care include ansamblul de acte, fapte și comportamente care deviază moral și legal de la îndatoririle oficiale ale exercitării unui rol public de către anumite persoane care exercită influență politică în sfera puterii în scopul obținerii unor avantaje personale. În cadrul corupției politice s-ar putea include și activitățile de finanțare și subvenționare ilegală a campaniilor electorale, cumpărarea de voturi cu ocazia alegerilor, acțiuni ilicite legate de unele partide clientelare sau punerea unor candidați pe listele electorale.

Cele trei forme ale corupției se intercondiționează și se potențează reciproc. De asemenea, din analizarea, chiar și sumară a celor trei forme principale ale corupției, rezultă legătura indisolubilă dintre corupție și crimă organizată.

Astfel, în lupta dusă de către instituțiile statului împotriva corupției trebuie avută permanent în vedere relația dinamică, bazată pe complementaritate și simbioză, dintre corupție și crima organizată.

CADRUL LEGISLATIV

În sistemul de drept românesc au intrat în vigoare, în ultimii ani, o serie de acte normative extrem de importante ce vizează prevenirea și combaterea fenomenului corupției. Astfel, *Convenția penală privind corupția* și *Legea nr. 78/2000* reprezintă instrumente moderne și eficiente de luptă împotriva corupției, pe plan național și internațional.

Convenția penală cu privire la corupție, adoptată la 27 ianuarie 1999 de statele membre ale Consiliului Europei, statuează faptul că lupta împotriva corupției se realizează printr-o cooperare internațională penală intensificată. Necesitatea de a urma cu prioritate o politică penală comună

tinde să protejeze societatea împotriva corupției, inclusiv prin adoptarea unei legislații și a măsurilor preventive adecvate, armonizate, de către statele semnatare ale Convenției.

În prevederile Convenției se definesc actele de corupție — *corupția pasivă* și *corupția activă*, evidențiindu-se corupția din sfera publică și corupția din sectorul privat, se nominalizează persoanele care pot avea calitatea de subiect activ al actelor de corupție, inclusiv cetățenii străini, funcționarii internaționali, membrii adunărilor parlamentare internaționale, judecătorii și agenții curții internaționale.

Se mai stipulează incriminarea traficului de influență, atât în modalitatea primirii, solicitării sau acceptării ofertei sau promisiunii, cu titlu de remunerație, pentru a exercita o influență în luarea unei decizii, cât și în modalitatea propunerii, oferind, direct sau indirect, un folos necuvenit persoanei care afirmă sau confirmă că este capabil să exercite o influență în luarea unei decizii de către agenții publici naționali.

De asemenea, se prevede în Convenție incriminarea acțiunilor de spălare a veniturilor provenite din delicte de corupție, fraudele în contabilitate legate de corupție și răspunderea pentru comiterea faptelor în cauză și sancționarea celor vinovați. Totodată, în această Convenție se prevede cooperarea în lupta cu corupția în plan național și internațional, inclusiv în efectuarea măsurilor de colectare a probelor, aplicarea sechestrului, protecția celor care colaborează cu autoritățile în investigarea cazurilor de corupție și a martorilor, extrădarea și alte aspecte privind combaterea acestui fenomen infracțional.

Legea nr.78 din 2000 privind prevenirea, descoperirea și sancționarea faptelor de corupție respectă cadrul general impus de către prevederile Convenției. Astfel, sunt incriminate ca infracțiuni de corupție: luarea și darea de mită, traficul de influență și primirea de foloase necuvenite. Sunt prevăzute de asemenea categoriile de persoane care sunt susceptibile de a săvârși astfel de infracțiuni (art.1,7,8).

De asemenea, sunt incriminate infracțiuni asimilate infracțiunilor de corupție, infracțiuni care exced prevederile

Convenției, asigurând un plus de eficacitate legislației penale române.

Putem să exemplificăm aici infracțiunea de efectuare de operațiuni financiare, cu acte de comerț, incompatibile cu funcția, atribuția sau însărcinarea pe care o îndeplinește o persoană, ori încheierea de tranzacții financiare, utilizând informațiile obținute în virtutea funcției, atribuției sau însărcinării sale; infracțiunea de folosire, în orice mod, direct sau indirect, de informații ce nu sunt destinate publicității, ori permiterea accesului unor persoane neautorizate la aceste informații; infracțiunea de acordare de credite sau de subvenții cu încălcarea legii sau a normelor de creditare, neurmărirea, conform legii sau normelor de creditare, a destinațiilor contractate ale creditelor sau subvențiilor, ori neurmărirea creditelor restante; infracțiunea de utilizare a creditelor sau subvențiilor în alte scopuri decât cele pentru care au fost acordate, toate acestea săvârșite în scopul obținerii pentru sine sau pentru altul de bani, bunuri sau alte foloase necuvenite.

În conformitate cu dispozițiile Convenției sunt incriminate infracțiuni în legătură directă cu infracțiunile de corupție; dintre acestea exemplificăm falsul și uzul de fals pentru a săvârși sau a ascunde săvârșirea unei noi infracțiuni de corupție ori a unei infracțiuni asimilate, ori spălarea banilor, atunci când banii, bunurile sau alte valori provin din săvârșirea unei infracțiuni de corupție ori a unei infracțiuni asimilate.

Legea privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și mediul de afaceri, prevenirea și sancționarea corupției, reprezintă o inițiativă complexă în lupta împotriva corupției. Principalele reglementări se referă la: (TITLUL I)

Transparența informațiilor referitoare la obligațiile bugetare restante; (TITLUL II) Transparența în administrarea informațiilor și serviciilor publice prin mijloace electronice; (TITLUL III) Prevenirea și combaterea criminalității informatice; (TITLUL IV) Conflictul de interese și regimul incompatibilităților în exercitarea demnităților publice și funcțiilor publice; (TITLUL V) Grupurile de interese economice.

Modificarea unor reglementări în scopul prevenirii și combaterii corupției fac referire la: (TITLUL I) Asigurarea transparenței în exercitarea funcțiilor publice, prevenirea și combaterea corupției; (TITLUL II) Asigurarea transparenței și stabilității în mediul de afaceri; (TITLUL III) Reglementări privind funcția publică și funcționarii publici.

Pe lângă acestea, în sistemul legislativ românesc mai sunt în vigoare și alte legi importante destinate prevenirii și combaterii fenomenului corupției, inițiate ca urmare a obligațiilor internaționale asumate de statul român la care vom face referiri în cele ce urmează.

Astfel, *Legea nr.682/2002 privind protecția martorilor*, elaborată de Ministerul Justiției împreună cu Ministerul Administrației și Internelor, este menită a reflecta responsabilitatea statului în asigurarea securității martorilor și garantarea posibilității lor de a depune mărturie în cauzele penale privind infracțiunile grave, în care depozițiile lor sunt determinante în aflarea adevărului. Această lege contribuie la armonizarea legislației interne cu o serie de documente internaționale printre care amintim: - *Recomandarea R(97) a Consiliului Europei, privind intimidarea martorilor și drepturile apărării; Rezoluția Consiliului Uniunii Europene din 20 decembrie 1996, privind persoanele care cooperează în procesul judiciar în lupta împotriva criminalității organizate; Rezoluția Consiliului Uniunii Europene din 23 noiembrie 1995, privind protecția martorilor în lupta împotriva criminalității internaționale organizate.*

Legea Nr. 39/2003 privind prevenirea și combaterea criminalității organizate a fost promulgată ca urmare a semnării de către statul român, la 14 decembrie 2000, la Palermo a: Convenției Națiunilor Unite împotriva criminalității transnaționale organizate; Protocolului adițional privind prevenirea, reprimarea și pedepsirea traficului de persoane, în special a femeilor și a copiilor; Protocolului adițional împotriva traficului de migranți pe calea terestră, a aerului și pe mare.

În vederea reprimării actelor de criminalitate organizată se impune, pe lângă ratificarea Convenției Națiunilor Unite

împotriva criminalității transnaționale organizate și a celor două protocoale adiționale semnate de România, elaborarea unui act normativ care să asigure, pe de o parte, crearea cadrului juridic corespunzător în domeniu, iar pe de altă parte, transpunerea în dreptul intern a prevederilor documentelor juridice internaționale menționate.

Legea nr. 656/2002 pentru prevenirea și sancționarea spălării banilor ține seama de recomandarea organismelor internaționale adresată guvernelor de a intensifica lupta împotriva spălării banilor prin sporirea și diversificarea mijloacelor de prevenire și combatere a acestui fenomen, inclusiv a mijloacelor juridice. Legea contribuie la armonizarea legislației interne cu: Convenția Europeană privind spălarea, depistarea, sechestrarea și confiscarea produselor infracțiunii, ratificată de România prin Legea nr. 253/2002; Convenția Organizației Națiunilor Unite împotriva criminalității organizate transnaționale, ratificată prin Legea nr.565/2002. Aceasta ține seama de recomandările Subcomitetului de experți pentru evaluarea măsurilor de combatere a spălării banilor din cadrul Consiliului Europei.

Adoptarea *Legii nr. 468/2002 privind achizițiile publice prin licitații electronice* a avut drept scop stabilirea principiilor, cadrului general și a condițiilor de utilizare a procedurii on-line pentru atribuirea contractelor de achiziție publică, precum și a regulilor generale de asigurare prin mijloace electronice a transparenței în domeniul achizițiilor publice.

Ordonanța de urgență nr.27 din 18 aprilie 2003, privind procedura aprobării tacite reglementează procedura aprobării tacite ca modalitate alternativă de emitere sau reînnoire a autorizațiilor de către autoritățile administrației publice, având la bază următoarele obiective:

a) înlăturarea barierelor administrative din mediul de afaceri;

b) responsabilizarea autorităților administrației publice în vederea respectării termenelor stabilite de lege pentru emiterea autorizațiilor;

c) impulsonarea dezvoltării economice prin oferirea unor condiții cât mai favorabile întreprinzătorilor, implicând costuri de autorizare cât mai reduse;

d) combaterea corupției prin diminuarea arbitrarului în decizia administrației;

e) promovarea calității serviciilor publice prin simplificarea procedurilor administrative.

Înființarea prin Ordonanța de Urgență a Guvernului nr.43/2002, aprobată prin Legea nr.503/2002, a *Parchetului Național Anticorupție*, ca structură specializată în prevenirea și combaterea infracțiunilor de corupție, răspunde cerințelor perioadei de tranziție pe care o parcurgem, fiind în concordanță cu dispozițiile constituționale, care privesc locul și rolul statului, al serviciilor publice și private în asigurarea unui cadru economic, social și politic corespunzător.

Asigurarea condițiilor necesare funcționării acestei noi structuri, corelarea actului normativ în cauză cu dispozițiile Codului penal, Codului de procedură penală, precum și ale altor legi speciale în materie, în mod deosebit ale Constituției, tratatelor și convențiilor la care România a aderat, vor fi de natură să ducă la înfăptuirea scopului propus.

Parchetul Național Anticorupție este conceput ca principală instituție care trebuie să lupte împotriva corupției, în vederea asigurării unui mediu social, economic și politic sănătos.

Potrivit Convenției penale privind corupția, ratificată prin Legea nr.27/2002, lupta împotriva corupției a căpătat dimensiuni internaționale, în care Parchetul Național Anticorupție, ca autoritate independentă specializată, îi revin sarcini deosebite.

Înființarea Parchetului Național Anticorupție împreună cu noutățile juridice cuprinse în Ordonanța de Urgență a Guvernului nr.43/2002, se înscriu pe coordonatele unei adevărate reforme în justiție.

Concret, *programe anticorupție derulate sau în curs de derulare* se află în responsabilitate la:

a) Ministerul Justiției — Programul RO 9910.05 de întărire a capacității instituțiilor statului, de luptă împotriva corupției și criminalității organizate; Programul Phare 2003; Programul OECD; Programul PACO SIMS;

b) Ministerul Public — Programul Tempus Phare;

c) Ministerul Administrației și Internelor — Programul „Restructurarea Ministerului de Interne și lupta împotriva crimei organizate"; Programul „Dezvoltarea mecanismelor anti-corupție";

CONCLUZII

Fără o abordare frontală și eficientă și fără sprijinul societății civile, care trebuie să se implice mai mult în actul de influențare a deciziilor politice, corupția poate deveni o formă letală pentru orice tip de activitate în România. Astfel, trebuie acceptat că într-o societate democratică cu o adevărată economie de piață, toți cetățenii și toți agenții economici sunt egali, indiferent de mărimea lor, iar legea trebuie respectată de către toți.

Riscurile abaterii de la regulile firești ale democrației și ale economiei de piață pot influența grav toate domeniile societății românești și, de aici, neîncredere politică, rezerve și suspiciuni din partea Uniunii Europene.

România nu poate pierde oportunitățile venite în conjunctura istorică de a se integra în UE și oricât de greu ar fi, așa cum spunea în istoria politicii lumii, cardinalul de Retz „politica este arta de a alege în momente dificile", iar factorii de decizie din România de azi, au oferit și oferă permanent certitudinea alegerii definitive și irevocabile a orientării euro-atlantice.

CORUPȚIA — RISC MAJOR LA ADRESA SECURITĂȚII NAȚIONALE

Mr. Magistrat Marian Lazăr

Corupția constituie o amenințare pentru democrație, pentru supremația dreptului, echității sociale și a justiției, erodând principiile unei administrații eficiente, subminând economia de piață și punând în pericol stabilitatea instituțiilor statale. Experiența românească din ultimul deceniu demonstrează că majoritatea acțiunilor anticorupție, s-au concretizat, în principal, în măsuri de combatere, al căror efect nu a fost nici pe departe cel scontat, după cum se arată în Programul național de prevenire a corupției, elaborat de Guvernul României.

Corupția, în sens larg, ca și corupția penală, în special, scoate în evidență aceeași atitudine față de etică și pentru a merge la esență trebuie precizat că, în toate situațiile, ea ține de abuzul de putere și de incorectitudinea în luarea unei decizii la nivel public.

În esență, corupția reprezintă utilizarea abuzivă a puterii publice în scopul obținerii pentru sine ori pentru altul, a unui câștig necuvenit implicând: abuzul de putere în exercitarea atribuțiilor de serviciu; frauda (înșelăciunea și prejudicierea unei alte persoane sau entități); utilizarea fondurilor ilicite în finanțarea partidelor politice și a campaniilor electorale; favoritismul; instituirea unui mecanism arbitrar de exercitare a puterii în domeniul privatizării sau al achizițiilor publice; conflictul de interese (prin angajare în tranzacții sau dobândirea unei poziții ori a unui interes comercial care nu este compatibil cu rolul și îndatoririle oficiale).

Potrivit Convenției penale a Consiliului Europei privind corupția, semnată de România la data de 27.01.1999, această activitate infracțională este definită în cele două modalități de săvârșire:

– *corupția activă* — „promisiunea, oferirea sau darea cu intenție, de către orice persoană, direct sau indirect, a

oricărui folos necuvenit, către un funcționar pentru sine sau pentru altul, în vederea indeplinirii sau abținerii de a îndeplini un act în exercițiul funcțiilor sale";

– *corupția pasivă* — „solicitarea ori primirea, cu intenție, de către un funcționar public, direct sau indirect, a unui folos necuvenit, pentru sine sau pentru altul, sau acceptarea unei oferte sau promisiuni a unui astfel de folos, în vederea îndeplinirii sau abținerii de a îndeplini un act în exercițiul funcțiilor sale".

În țările aflate în tranziție, fenomenul corupției își are proveniența într-o multitudine de factori de natură politică, economică și socială: nivelul inițial de dezvoltare; moștenirea politică, economică și instituțională; înzestrarea naturală și socială; opțiunile politico-instituționale; nivelul competiției politice și al concentrării economice.

ETIOLOGIA CORUPȚIEI ÎN ROMÂNIA

În vechiul drept penal românesc, corupția este incriminată destul de târziu și limitat în perioada domniilor fanariote.

Faptele de corupție constau în daruri făcute de către subalterni sau de către particulari, dregătorilor, în dubla lor calitate de funcționari și judecători. Începând cu perioda fanariotă, moravurile impuse de către demnitarii fanarioți au înlocuit obiceiurile austere ale poporului român și au condus la generalizarea corupției, atât în raporturile cu demnitarii turci, cât și în cele dintre funcționarii români, ori între aceștia și populație.

Lionardo Panzini, fost perceptor al fiilor lui Alexandru Ipsilanti scria odată că „miniștrii de lângă domn știu să facă întocmai ce face el. Toți slujbașii au grijă să le urmeze pilda, întrucât, întreaga cârmuire nu este altceva decât un jaf; toți membrii ei sun niște lipitori dornice să sugă ultima picătură de sânge a unor mulțimi vlăguite. Nici unul dintre evenimentele care au înrâurit existența politică și care au distrus

spiritul public al moldovenilor și valahilor n-a fost atât de dezastruos ca sistemul de politică introdus de Fanar. Totul este păstrat cu grijă și trimis la Stambul, unde vor fi plătiți prietenii, ocrotitorii domnului care, astfel, își pregătește propriile izbânzi".

De-a lungul timpului au apărut reglementări în materie penală prin care s-a încercat stăvilirea actelor de corupție însă rezultatele nu au fost nici pe departe cele scontate. Dintre acestea amintim Condica de drept penal și procedură penală intrată în vigoare la 1ianuarie 1852, în Muntenia, sub domnia lui Barbu Știrbei, precum și codurile penale din 1865, 1936 și 1968.

În perioda recentă, oportunitățile oferite de fenomenul de tranziție coroborate cu insuficiența și ineficiența controlului statal au favorizat dezvoltarea actelor de corupție, în special a criminalității economice, orientată spre obținerea de profituri maxime.

Potrivit Strategiei de prevenire și control social al corupției au fost identificate două niveluri ale acestui fenomen infracțional, fiind adoptate măsuri specifice: marea corupție; mica corupție.

„Marea corupție" este asociată funcțiilor de nivel înalt, factorilor de decizie majoră, formelor grave de fraudă, extorcări de fonduri și nu în ultimul rând criminalității organizate, în timp ce „mica corupție" are cel mai puternic impact pentru opinia publică.

În legislația anticorupție din țara noastră, distincția dintre cele două niveluri ale corupției are la bază un sistem complex de factori constând în calitatea persoanei vizate, valoarea sumei sau bunului ce formează obiectul infracțiunii de corupție și cuantumul pagubei materiale cauzate prin infracțiunea respectivă.

Clasificarea are în vedere influențarea actelor normative în timpul elaborării sau aplicării lor, astfel: *state capture* — desemnează acțiunile unor grupuri, persoane sau firme din sectorul public sau privat — realizate în scopul de a influența în interes propriu conținutul unei legi; *corupția administra-*

tivă — distorsionarea intenționată a aplicării legilor, normelor și reglementărilor pentru a creea avantaje unor actori publici sau privați, prin acordarea de câștiguri personale unor oficialități, pe căi ilicite sau alte mecanisme netransparente.

MĂSURI LEGISLATIVE PENTRU PREVENIREA ȘI COMBATEREA CORUPȚIEI

Globalizarea fenomenului corupției, diversificarea formelor și tipurilor corupției, precum și implicațiile nefaste ale acesteia asupra sistemelor sociale, au impus conceperea și elaborarea unor strategii adecvate de prevenire și combatere.

Astfel, pe plan internațional, european și național au fost adoptate numeroase acte normative, încercându-se stăvilirea și controlarea acestui fenomen. În plan intern, actul normativ cadru în acest domeniu este Legea nr. 78/2000 privind prevenirea, descoperirea și sancționarea faptelor de corupție.

Pornind de la legislația existentă în unele țări europene (Italia, Spania, Germania), precum și de la necesitatea realizării în România a unei structuri judiciare specializate în combaterea corupției, a fost creat Parchetul Național Anticorupție ca o structură autonomă în cadrul Ministerului Public, ce-și exercită atribuțiile la nivel național pentru combaterea „marii corupții".

Datorită mijloacelor moderne de comunicare și a unei mari deschideri a frontierelor în Europa manifestările crimei organizate au căpătat un caracter transnațional, desfășurându-se de cele mai multe ori pe fondul coruperii unor funcționari publici cu atribuții judiciare sau financiare, ori a unor funcționari vamali.

În țările europene, domeniile în care activitățile infracționale au loc pe fondul unor acte de corupție sunt următoarele: activitatea antreprizelor; contrabanda de țigări; evaziunea fiscală; spălarea banilor; comercializarea ilegală

a alcoolului; falsificarea cărților de credit; transferuri frauduloase de bani prin mijloace electronice; traficul de deșeuri și infracțiunile cu incidență asupra mediului înconjurător; traficul de arme și muniții, materiale nucleare, droguri sau ființe umane; deturnarea și schimbarea destinației subvențiilor.

În țara noastră au fost identificate următoarele forme de corupție: corupția administrativă; corupția în justiție; corupția economică; corupția politică.

Tendințele de creștere a actelor și faptelor de corupție în societatea românească reprezintă un fenomen real ale cărui efecte nu pot fi ignorate nici de criminologi și sociologi și nici de instituțiile specializate în domeniul aplicării legilor, respectiv, apărării legalității și ordinii de drept.

În perioada de tranziție pe care o parcurge România, agravarea unor probleme sociale, între care și corupția, se datorează în bună măsură ineficienței unor reglementări normative, slăbirii mecanismelor de control social realizate prin lege și justiție, ambivalenței criteriilor de apreciere și sancționare a infractorilor, multiplicării și perfecționării mijloacelor infracționale pentru atingerea scopurilor ilicite de către anumiți indivizi și grupuri în procesul accesului spre statuturi superioare, bogăție, prestigiu și putere.

Etapa actuală din România se caracterizează printr-o amplificare fără precedent a manifestărilor de devianță sub toate formele sale, de la conduitele inofensive care frizează dacă nu patologicul, oricum grotescul, până la actele cu caracter penal ce evoluează și ele pe un continuum, de la delictele mai puțin grave, până la infracțiunile cu periculozitate sporită comise contra integrității persoanei prin agresivitate și violență sau împotriva patrimoniului public și privat.

Pe aceeași coordonată se constată și o intensificare a actelor de corupție care implică înalți funcționari ai statului, respectiv, creșterea numărului infracțiunilor economice incluzând fapte de fraudă, dare și luare de mită, primire de foloase necuvenite, trafic de influență, evaziune fiscală, tranzacții financiare și comerciale dubioase, etc.

Totodată, traficul de materii prime vândute în străinătate, transferul ilegal de capital și bunuri, traficul de persoane, comerțul ilicit cu mașini, traficul de arme, muniții și droguri, cazurile de corupție semnalate zilnic în presă sau de opinia publică, ori constatate de organele judiciare demonstrează fără nici un dubiu că în România s-au pus deja bazele unor rețele ale crimei organizate, cu ramificații atât în străinătate cât și pe plan intern, mergând până la cele mai înalte nivele ale administrației, justiției și puterii de stat.

Apare clar că frecvența ridicată a actelor de corupție nu se datorează doar transparenței statisticilor justiției, ori semnalelor presei și opiniei publice, ci unor tendințe și mecanisme care se află chiar în inima sistemului, în starea de criză care însoțește, ceea ce într-un cuvânt, atât de dătător de speranță pentru unii, ori detestabil pentru alții, se numește tranziția către economia de piață, ce constituie pilonul fundamental al unei societăți democratice.

În momentul de față se pun o serie de întrebări, se avansează ipoteze de lucru, se caută soluții și măsuri și se încearcă, pe cât posibil, concentrarea eforturilor în direcția identificării cauzelor și condițiilor care determină sau favorizează amplificarea corupției în diferite sectoare de activitate economică, socială, politică și administrativă.

Ținând seama de amploarea și diversificarea fenomenului corupției, autoritățile române au adoptat o stategie națională anticorupție materializată în Programul național de prevenire a corupției și Planul național de acțiune împotriva corupției, adoptate pri H.G. nr. 1065/2001.

Din aceeași necesitate a fost adoptată și Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției. Analiza acestiu fenomen infracțional evidențiază faptul că, stadiul actual al corupției în România reprezintă unul dintre pricipalele obstacole în calea integrării europene și a relansării economice prin atragerea investitorilor străini, astfel

că, putem concluziona că, „plaga corupției" constituie o amenințare la adresa securității naționale.

Corupția reprezintă un factor de injustiție socială care întreține și amplifică sărăcia, afectând în ultimă instanță dezvoltarea economică, aceasta fiind cea mai credibilă și temeinică sursă de securitate.

În prezent, corupția poate fi considerată ca fiind un fenomen deosebit de grav ce atacă bazele societății românești, pune în pericol stabilitatea instituțiilor statale și afectează nivelul de trai al populației prin creșterea nejustificată, de multe ori în mod dramatic, a costurilor sociale.

Pe termen scurt și mediu diversele forme de manifestare a riscului corupției ar putea avea următoarele consecințe negative la adresa securității naționale: pierderea credibilității României ca țară angajată ferm către integrarea euroatlantică, în special sub aspectul capacității de a utiliza deplin și efectiv fondurile Uniunii Europene și de a proteja interesele financiare ale comunității împotriva fraudei și corupției; dezorganizarea sistemelor de conducere și de execuție, respectiv dereglarea mecanismelor administrative, juridice și economice; eșecul procesului de reformă; sporirea costurilor sociale și sărăcirea populației; scăderea moralului populației și erodarea increderii în factorii de conducere, justiție și administrație; perturbarea funcționării sistemelor de furnizare a serviciilor edilitare esențiale.

MODALITĂȚI DE PREVENIRE ȘI COMBATERE A CORUPȚIEI ÎN ROMÂNIA

La nivelul anului 2004, Guvernul României apreciază că în domeniul instituțional, principalele direcții de luptă împotriva corupției sunt:

– reducerea rolului statului prin diminuarea puterii sale discreționare. Aceasta se poate efectua, fie prin liberalizare, fie prin introducerea unor noi reguli implicite, cu caracter automat;

– responsabilizarea instituțiilor în fața cetățenilor prin obligarea guvernului și a tuturor funcționarilor publici să informeze societatea civilă cu privire la activitățile lor și să ia atitudine în cazurile în care serviciile unor funcționari nu sunt satisfăcătoare;

– flexibilizarea structurilor instituționale și cointeresarea funcționarilor din aparatul de stat în lupta împotriva corupției;

– încheierea procesului de reformă în justiție.

În concluzie, pentru o soluție simplă, de etapă, exercitarea unui control direct, eficient și responsabil asupra activității fiecărui funcționar public este premisa limitării abuzului de putere și pe cale de consecință a corupției.

Totodată, o economie de piață viabilă va face să funcționeze și un sistem administrativ, iar la rândul său, funcționarea acestuia va fi limitată în baza legii doar de o justiție independentă.

De asemenea, în scopul prevenirii și limitării fenomenului corupției se impune cu necesitate implementarea următoarelor soluții:

– adoptarea unor coduri de conduită și deontologice pentru anumite categorii de funcționari publici și a unor planuri sectoriale pentru fiecare domeniu vulnerabil la corupție;

– modificarea legislației privind finanțarea partidelor politice și a campaniilor electorale;

– perfecționarea sistemului de selectare, promovare și evaluare periodică a funcționarilor publici;

– reforma managementului în sistemul public și a sistemului instituțional;

– realizarea unui parteneriat al autorităților publice cu societatea civilă și reprezentanții sectorului privat;

– invitarea societății civile pentru a supraveghea desfășurarea activităților vulnerabile la corupție, cum ar fi privatizările și achizițiile publice importante;

– educarea cetățenilor cu privire la cauzele și consecințele corupției, precum și la drepturile cetățeanului în situația când se confruntă cu cazuri de corupție;

– cooperarea între componentele sistemului național de securitate în domeniul prevenirii și combaterii corupției.

Reformele în acest domeniu sunt de competența politicului. Esențial în elaborarea unei strategii anticorupție care să acționeze fie în sectorul public, fie în cel privat, este voința politică.

Fenomenul corupției reprezintă un risc la adresa securității naționale, fapt demonstrat de amploarea și dezvoltarea corupției, această realitate nocivă fiind reflectată în reacțiile oficiale, inclusiv în legislație și în percepția opiniei publice. În aceste condiții, fenomenul corupției reprezintă un adevărat obstacol în cale promovării intereselor naționale ale României. Pricipala consecință a considerării corupției ca reprezentând un risc la adresa securității naționale o reprezintă necesitatea unei reacții ferme din partea tuturor forțelor sociale și, mai ales, din partea instituțiilor care asigură conducerea în domeniul securității naționale.

De asemenea, considerarea corupției ca factor de risc s-ar putea reflecta în conținutul celorlalte acte normative ce vizează apărarea națională și siguranța națională și ar eficientiza măsurile dispuse pentru contracararea altor factori de risc la adresa securității naționale.

În plus, acestă abordare ar deschide drumul unor măsuri drastice în acest domeniu și ar da posibilitatea implicării tuturor instituțiilor publice și cetățenilor în lupta împotriva corupției, cu consecințe directe asupra dezvoltării economice și a securității cetățenilor României. În caz contrar, corupția va deveni o amenințare la adresa securității naționale, iar caracterul său generalizat și instituționalizat va afecta sectoare vitale ale economiei, administrației, justiției și vieții politice cu consecințe nefaste incalculabile pentru viitorul României.

BIBLIOGRAFIE SELECTIVĂ

Strategia de securitate națională a României.

Legea nr. 51/1991 privind siguranța națională a României.

Legea nr. 14/1992 privind organizarea şi funcţionarea Serviciului Român de Informaţii.

Legea nr. 415/2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării.

Legea nr. 78/2000 pentru prevenirea, descoperirea şi sancţionarea faptelor de corupţie.

H.G. nr. 1065/2001 privind aprobarea Programului naţional de prevenire a corupţiei şi a Planului naţional de acţiune împotriva corupţiei.

Ordonanţa de Urgenţă nr. 43/2002 privind Parchetul Naţional Anticorupţie, aprobată prin Legea nr. 503/2002 şi modificată prin Legea nr. 161/2003.

Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei.

Convenţia asupra corupţiei a Consiliului Europei din anul 1999.

Vasile Dobrinoiu, *Corupţia în dreptul penal român*, Editura ROMFEL, Bucureşti 1995.

Tudor Amza, *Criminologie teoretică*, Editura LUMINA LEX, Bucureşti 2000.

Dan Banciu, Sorin Rădulescu — Corupţia şi crima organizată în România, Editura CONTINENT XXI, Bucureşti 1994.

Franco Roberti, *Cooperarea judiciară în combaterea criminalităţii organizate şi a criminalităţii economice*, material apărut în *culegerea „Lupta împotriva corupţiei şi criminalităţii organizate"*, editată în anul 2001 de Ministerul Public — Centrul de pregătire continuă a procurorilor.

Rodica Stănoiu, Hortansa Brezeanu, Tiberiu Dianu, *Tranziţia şi criminalitatea*, Editura OSCAR PRINT, Bucureşti 1994.

Dan Banciu, Sorin Rădulescu, Vasile Teodorescu, *Tendinţe actuale ale crimei şi criminalităţii în România*, Editura LUMINA LEX, Bucureşti 2002.

ELEMENTE ALE UNEI STRATEGII ANTICORUPȚIE EFICIENTE

Nelu Coman

Corupția reprezintă, în cea mai simplă descriere a sa, abuzul de putere, cel mai adesea în scopul obținerii de câștiguri personale sau în avantajul unui grup căruia cineva îi este devotat. Corupția poate fi motivată de lăcomie, de dorința de păstrare sau de sporire a puterii sau credința într-o presupusă stare de mai bine. Deși cel mai adesea cuvântul „corupție" este asociat abuzului de putere politică din partea politicienilor sau funcționarilor publici, acest concept descrie, de fapt, un tipar comportamental întâlnit în aproape orice sector.

Corupția este un fenomen complex, care își are rădăcinile în istoria socio-culturală a unei țări, în dezvoltarea sa politică și economică și în politicile și tradițiile sale birocratice. Generalizând, corupția are tendința de a înflori acolo unde instituțiile sunt slabe, iar politicile economice sunt defavorabile pieței.

Combaterea corupției a devenit una dintre principalele preocupări ale comunității internaționale. După ce ani la rândul a fost privită ca un subiect tabu, corupția devine o adevărată preocupare și pentru securitatea națională.

Combaterea corupției nu reprezintă un scop în sine. Acest proces este mai degrabă un instrument ce asigură o guvernare mai eficientă și mai corectă, asociată la rândul său cu un nivel superior de dezvoltare economică. Activiștii anticorupție nu sunt preocupați doar de corupție, ci și de impactul acesteia asupra dezvoltării și societății. Cum reușește corupția să obstrucționeze procesul de eliminare a sărăciei prin compromiterea deciziilor care ar putea conduce la dezvoltare? Cât de ineficientă este mita? Cine plătește până la urmă costurile corupției?

Deși existența corupției implică o serie de costuri importante, încercarea de a o elimina în totalitate nu este cea mai

fericită opțiune. Realist vorbind, în multe situații, reducerea la zero a corupției ar presupune costuri prea mari, iar acest proces ar afecta în mod inacceptabil drepturile fundamentale ale omului, precum și alte libertăți. De asemenea, eliminarea programelor ar putea fi nejustificată, birocrația discreționară ar putea fi necesară pentru o administrație eficientă, iar intensificarea constrângerilor și a restricțiilor ar putea fi o măsură pe care societatea să nu și-o poată permite. Astfel, scopul final nu ar trebui să fie eradicarea completă a corupției ci, mai curând, sporirea integrității guvernului și implicit a eficienței și corectitudinii acestuia.

Condițiile generale variază considerabil de la o societate la alta, dar reacțiile la fenomenul corupției, în ceea ce privește politicile, se încadrează, în general, în trei categorii: faptice, structurale și morale. Luate individual sau împreună, aceste reacții exprimă interesele și implicarea guvernului, sectorului privat și societății civile.

O analiză a succeselor (destul de rare) și a eșecurilor (numeroase) cu care s-au soldat în trecut eforturile de combatere a corupției în diverse țări conduce la identificarea unor elemente cheie ce pot constitui obstacole în calea succesului unei strategii anticorupție:

Autoritate limitată la vârf. Este posibil ca o nouă administrație să dorească o abordare eficientă a corupției, dar moștenirea unei birocrații corupte ar putea constitui un obstacol în calea eforturilor de schimbare.

Neimplicarea liderilor. Adesea, liderii nu au demonstrat un angajament suficient de serios. Promisiunile exagerat de ambițioase au generat așteptări nerealiste și greu de împlinit, care au condus la pierderea încrederii publicului.

Reforme parțiale, prost coordonate. Este cazul când nimeni nu își asumă reformele, nu se angajează să le ducă la îndeplinire și nu are motivația de a le vedea implementate și permanent actualizate.

O încredere exagerată în remediile juridice. Modificarea legilor și îmbunătățirea aplicării acestora este o strategie nesigură pentru a schimba comportamentul oamenilor. Iar

o încredere exagerată în aplicarea legilor conduce la represiune, la abuzul de putere și la apariția unui număr mai mare de cazuri de corupție.

Concentrarea numai asupra „peștilor mici". În această situație, reformele îi trec cu vederea pe cei aflați în vârf. Dacă legea este văzută ca fiind aplicată neuniform și incorect, curând nu i se va mai acorda nici cea mai mică atenție.

Lipsa unui obiectiv precis și realizabil. Reformele care nu produc „rezultate rapide" pierd repede sprijinul public. Chiar și atunci când reformele au avut un obiectiv precis și au generat schimbări reale, ele nu au durat dacă mecanismele instituționale nu au supraviețuit inițiatorilor reformelor.

Eșecul în implicarea partenerilor din afara guvernului. Mai presus de orice, o încercare a guvernului de a realiza reforme fără sprijinul reprezentanților societății civile și ai sectorului privat nu poate avea șanse de succes.

Deși costurile corupției sunt greu de măsurat, o serie de studii indică faptul că printre acestea se numără: o creștere de 3–10% a prețului unei tranzacții pentru a accelera furnizarea unui anumit serviciu guvernamental; prețuri crescute pentru anumite bunuri — cu până la 15–20% — ca urmare a monopolurilor impuse de guvern; o pierdere de până la 50% din impozitele percepute de guvern din cauza abuzurilor și corupției; costuri excesive aferente unor bunuri și servicii, din cauza supradimensionării prețului plătit pentru contractele de achiziții sau din cauza achiziționării unor articole scumpe și inutile, guvernele plătind cu 20–100% mai mult decât necesar.

Încercând să facem un calcul simplu, vom ajunge la pierderi uriașe la nivelul bugetului fără a ține cont de implicațiile sociale ale fenomenului, care, în mod sigur pot plasa problematica corupției în sfera interesului securității naționale.

Klitgaar a elaborat un model simplu care explică dinamica fenomenului corupției: *C* (corupție) = *PM* (puterea de monopol) + *CD* (control discreționar) — *R* (responsabilitate).

Dezvoltarea unei strategii coerente, generale și complexe implică un angajament clar din partea liderilor politici în

combaterea corupției, oriunde apare aceasta. Acest lucru înseamnă că liderii vor accepta să se supună unor controale. Experiența demonstrează că eforturile trebuie îndreptate în primul rând către prevenirea viitoarelor acte de corupție și către schimbarea sistemelor, renunțându-se la vânătoarea de vrăjitoare.

O legislație anticorupție amplă trebuie să fie adoptată și implementată de agenții cu o integritate recunoscută. Este prioritară identificarea acelor sectoare guvernamentale care sunt cel mai expuse la corupție, precum și revizuirea procedurilor relevante. Salariile funcționarilor publici și ale liderilor politici trebuie să reflecte responsabilitățile posturilor respective și să fie, pe cât posibil, comparabile cu cele din sectorul privat, atât pentru a reduce „necesitatea" actelor de corupție, cât și pentru ca statul să beneficieze de cei mai competenți angajați. „Remediile" juridice și administrative împotriva corupției trebuie să includă restricții adecvate (de exemplu, contractele obținute prin corupție să fie anulate, marile tranzacții atent monitorizate, să se instituie controale financiare inopinante și să se anuleze licențele și autorizațiile obținute prin metode corupte). Cel mai important lucru este stabilitatea unui parteneriat creati0v între guvern și societatea civilă, inclusiv sectorul privat, ligile profesionale, organizațiile neguvernamentale și așa mai departe.

Reformele se pot încadra în patru categorii: *prevenire, aplicare, informare publică și dezvoltare instituțională.* În fiecare situație, scopul final este transformarea corupției într-un act neprofitabil, care implică riscuri.

Simplificarea programelor și procedurilor guvernamentale contribuie la reducerea oportunităților de apariție a corupției. Cu cât planul ce stă la baza unui program este mai eficient, cu atât mai puțin va fi acesta mai expus corupției. Una dintre reforme este reprezentată de eliminarea celor care ocupă poziții ce le permit să solicite mită. O alta presupune reducerea numărului de etape necesare pentru a obține autorizații guvernamentale sau pentru a plăti pentru

bunurile solicitate. Ca urmare, simplificarea și aplicarea reglementărilor guvernamentale va diminua necesitatea de a plăti mită și va facilita realizarea tranzacțiilor în general.

Domeniile în care este permisă libertatea de acțiune vor fi reduse la maxim sau eliminate, acolo unde este posibil. Pentru cele care vor fi menținute, se vor elabora manuale și alte materiale asemănătoare. Coduri de comportament pentru angajați și alte asemenea materiale trebuie puse la dispoziția utilizatorilor din cadrul fiecărui departament și nu numai. Ocaziile de apariție a corupției pot fi reduse și prin clarificarea rolului pe care îl are guvernul, deoarece corupția prosperă acolo unde publicul nu este conștient de drepturile sale. Vor exista mai puține ocazii de utilizare a practicilor corupte dacă va fi redus cât mai mult contactul direct, conducând astfel la o depersonalizare a guvernului. Pot fi introduse elemente aleatorii, astfel încât cei care fac afaceri cu guvernul să nu poată anticipa cu cine vor avea de a face. O altă strategie de luat în considerare este rotirea personalului-cheie, ceea ce va reduce riscul dezvoltării unor relații nesănătoase între acesta și public, precum și în interiorul grupurilor de angajați guvernamentali.

Trebuie analizate mecanismele prin care se poate realiza o evaluare rapidă și eficientă a deciziilor controversate. Directorii de la toate nivelurile trebuie să fie responsabili pentru activitățile subordonaților. Eficiența procesului de supervizare poate fi amplificată împuternicindu-i pe superiori să treacă în revistă și să controleze activitatea personalului subordonat, prin controale de rutină și inopinante. De asemenea, directorii trebuie să certifice în mod regulat faptul că subordonații respectă legea și reglementările specifice serviciului civil. Trebuie să existe și un sistem de reclamații, care să le permită persoanelor de rang inferior să dezvăluie actele de corupție comise de superiori, iar presa trebuie să aibă libertatea de a scrie despre aceste cazuri.

Funcționarii publici trebuie să primească un salariu care să răspundă nevoilor și așteptărilor acestora. Trebuie intro-

dus sistemul recompensării pentru performanță și al exemplului pentru comportament. Este, de asemenea, necesară crearea unor mecanisme de implicare a societății civile, care să stea la baza procesului continuu de revizuire. Trebuie realizate sondaje de opinie periodice pentru a testa reacția publicului în legătură cu schimbările efectuate. În plus, veniturile, bunurile și datoriile oficialilor cu putere de decizie trebuie să fie atent monitorizate pentru a verifica dacă există o compatibilitate cu datele existente și cu așteptările firești ale publicului. Trebuie, de asemenea, instituite restricții referitoare la angajarea în sectorul privat.

Este importantă crearea unui sistem de achiziții publice deschis, transparent, cu adevărat concurențial. Pentru a consolida eforturile de combatere a corupției, asociațiile profesionale de contabili, controlori financiari și avocați trebuie să denunțe participarea la activități corupte (inclusiv spălarea banilor) și să-i sancționeze pe vinovați cu excluderea profesională. Ar trebui impusă raportarea tuturor cadourilor primite de oficialii guvernamentali, precum și raportarea și înregistrarea tuturor donațiilor politice.

De asemenea, este necesară revizuirea reglementărilor referitoare la conflictele de interese. Acest lucru implică introducerea unor programe de etică și organizarea periodică a unor dicuții de grup pe marginea unor dileme etice cu care s-au confruntat funcționarii publici în activitatea de fiecare zi. În anumite cazuri, este de dorit eliminarea anumitor activități din sfera serviciului public (de exemplu, constituirea unei autorități separate pentru venituri) astfel încât cei care lucrează în domenii sensibile să poată primi salarii mai mari fără ca acest lucru să influențeze în vreun fel serviciul public. La fel de importantă este eliminarea „monopolurilor" birocratice pentru crearea unor surse concurente de servicii, punând astfel capăt tarifelor neoficiale sau cel puțin coborând valoarea acestora.

În cele din urmă, trebuie construite coaliții de interese pentru a sprijini prevenirea corupției. Aceste coaliții trebuie

să implice atât sectorul privat, cât și societatea civilă, iar în anumite cazuri, ele pot organiza campanii de informare publică în scopul diminuarii toleranței față de corupție.

Trebuie implementate mecanisme independente de aplicare a măsurilor, pentru a crește probabilitatea identificării și pedepsirii actelor de corupție. Anchetatorii, procurorii și judecătorii trebuie să aibă capacitatea de a-și îndeplini îndatoririle profesionale într-un mod transparent și independent și de a aplica legea în cazul tuturor celor care o încalcă, indiferent de funcțiile deținute de aceștia (depolitizând astfel aplicarea legii). Sunt deci necesare prerogative adecvate de anchetare și urmărire în justiție, în conformitate cu normele internaționale referitoare la drepturile omului. De exemplu, anchetatorii trebuie să aibă acces la toate documentele și dosarele guvernamentale gestionate de avocați și consilieri financiari. Trebuie dezvoltate acorduri mutuale internaționale de asistență juridică cu anumite țări, iar persoanele care dețin averi importante trebuie să demonstreze că acestea au fost acumulate în mod legal.

De asemenea, trebuie să existe prevederi care să instituie mecanisme treansparente pentru eliminarea imunității unor înalți oficiali care se bucură de acest privilegiu prin natura funcției. Trebuie instituite canale de transmitere a reclamațiilor, atât pentru informatorii din cadrul guvernului, cât și pentru public, deoarece este esențial ca nimeni să nu se simtă amenințat de posibile represalii. De exemplu, se pot crea linii telefonice speciale și servicii de consiliere (preferabil independente de serviciul civil). În plus, dacă este necesar, se poate asigura protecția fizică a informatorilor-cheie, atât în țară, cât și în afara ei. De asemenea, persoanele private care pierd bani sau contracte din cauza corupției trebuie să aibă dreptul de a cere despăgubiri în instanță.

Trebuie, de asemenea, puse la punct mecanisme de pedepsire a celor care se află în afara granițelor. O altă soluție este redactarea unor liste cu numele companiilor corupte, care includ și numele membrilor personalului din vânzări

care se face vinovat de acte de corupție, și publicarea acestor nume ca o modalitate de a informa alte țări sau companii concurente în legătură cu activitățile corupte ale persoanelor în cauză.

Trebuie încheiate acorduri de extrădare, astfel încât oficialii corupți care se refugiază în străinătate să poată fi deferiți justiției. Sunt necesare măsuri juridice care să permită confiscarea bunurilor persoanelor corupte, indiferent dacă se află în interiorul țării sau în afara ei.

Publicul trebuie să înțeleagă cât de dăunătoare este corupția și că cei vinovați de corupție nu fac decât să fure din banii publici. La fel de importantă este educarea cetățenilor în legătură cu drepturile lor la servicii — la un anume preț sau fără nici un fel de cost — precum și cu datoria de a face reclamații în legătură cu comportamentul corupt al oficialilor, respectând procedurile în vigoare. De asemenea, trebuie clarificată percepția publicului în legătură cu incidența cazurilor de corupție și localizarea acestora, pentru a stabili un reper în vederea evaluării ulterioare a progreselor realizate.

Pentru ca publicul să fie informat, structura administrativă și juridică trebuie să asigure existența unei prese libere. Nu trebuie să existe cenzură, iar guvernul nu trebuie să trateze presa într-un mod discriminatoriu. Trebuie făcute eforturi pentru a ridica standardele profesionale, asigurând în același timp, la nivelul companiilor de presă, prezența unor angajați care pot fi echidistanți și pot da dovadă de răspundere profesională.

În primul rând, toate instituțiile relevante trebuie să aibă un personal adecvat și resurse corespunzătoare. Un set de reguli și repere de conduită clare trebuie formulat și diseminat. Funcționarii publici trebuie să beneficieze de instruire la locul de muncă, iar nevoile de perfecționare profesională ale tuturor departamentelor și agențiilor relevante trebuie evaluate.

Sistemele de management financiar intern trebuie revizuite pentru a se asigura eficiența și compatibilitatea acestora.

Instituția supremă de control financiar trebuie să fie independentă, profesionistă și să dispună de un mecanism care să permită o selecție atentă a personalului; de asemenea, această instituție trebuie să aibă capacitatea de a genera rapoarte accesibile la nivel extins, precum și autoritatea de implementare a recomandărilor. Avocatul poporului trebuie, de asemenea, să aibă prerogative adecvate, inclusiv capacitatea de a-și face publică activitatea și rapoartele, precum și de a asigura o reacție la recomandările sale.

Domeniul achizițiilor trebuie să fie profesionalizat, printr-o comparație între practicile curente, pe de o parte, și practicile etalon și sistemele care beneficiează de un grad maxim de transparență, pe de altă parte. Alegerea nu trebuie să depindă exclusiv de opiniile și interesele departamentale; pot fi solicitate și persoane din exterior. Factorilor de decizie nu trebuie să li se dea ocazia de a anticipa cine va participa la o anumită acțiune. Deciziile trebuie luate rapid, pentru a elimina întârzierile în cursul cărora pot apărea cazuri de corupție. Procedurile departamentale trebuie evaluate periodic, precum și ori de câte ori apar reclamații.

Comisia pentru alegeri trebuie să fie independentă și imparțială pentru a se putea bucura de încrederea publicului și a partidelor politice, și trebuie să păstreze transparența în privința tuturor aspectelor sistemului electoral (desigur, cu excepția votului în sine). Comisia trebuie să încurajeze participarea publică la procesul de monitorizare pentru a consolida încrederea publicului, familiarizându-și, în același timp, personalul și pe reprezentanții partidelor cu anumite aspecte ale sistemului, și instruindu-i în vederea unei monotorizări profesioniste a acestuia.

Mecanismele legislative pentru asigurarea responsabilității, printre care se numără un comitet al conturilor publice, trebuie evaluate periodic și revizuite dacă este necesar. Accesul public la activitățile legislative trebuie intensificat la maxim. De asemenea, trebuie dezvoltată o modalitate de sondare periodică a opiniei publice. Atunci când apar acuzații

de corupție, activitățile de anchetare și urmărire în justiție trebuie desfășurate independent.

Reforma anticorupție este un proces pe termen lung, în cadrul căruia atitudinile și comportamentele adecvate se învață și se cultivă la toate nivelurile. La început, reformele trebuie aplicate numai acolo unde pot fi cel mai eficiente și unde pot aduce o contribuție valoroasă. Procedul de reformă trebuie să fie vizibil "adoptat" și sprijinit de liderii statului. La final, lupta împotriva corupției are drept rezultat și întărirea încrederii și loialității publicului față de stat, precum și consolidarea capacității financiare și politice a statului de a-și servi cetățenii.

III. MIJLOACELE DE INFORMARE ȘI PROBLEMELE DE SECURITATE ȘI SIGURANȚĂ NAȚIONALĂ

MASS-MEDIA ȘI SIGURANȚA NAȚIONALĂ

Barbu Tudor

Articolul 1 din Legea nr. 51 — iulie 1991 — definește conceptul de Siguranță Națională a României așa cum a fost el identificat de legiuitor în contextul istoric dat.

Articolul 2 din aceiași Lege face precizarea: Siguranța Națională se realizează prin cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe ce pot aduce atingere valorilor fundamentale care o compun: legalitate, echilibru și stabilitate socială, economică, politică necesare existenței și dezvoltării statului național român suveran, unitar, independent și indivizibil.

Constituția României, cu tot ce decurge din litera și spiritul ei, poate opera numai în condițiile oferite de asigurarea unui climat de securitate colectivă în planurile individului și al instituțiilor.

Bun! Și — se poate întreba oricine — unde este legătura între presă și tot acest eșafodaj de prevederi legale și activități menite a asigura esențiala Securitate Națională?

Mass-media este într-adevăr o putere a statului și câinele de pază al societății dar...alții sunt cei abilitați, meniți și pregătiți să asigure României Securitatea Națională atât de necesară într-o perioadă istorică în care totul este în schimbare. Se modifică radical, la început de mileniu III, vectorii de amenințare și modalitățile de contracarare, se schimbă ordinea economică mondială și — odată cu ea — legile „războiului" globalizării, apar noi „arme" politice la scară macro și se sapă noi „tranșee" de rezistență la nivelul fiecărui stat.

Presa are rolul ei dar nu poate și, ar merge unii mai departe, nu trebuie să fie implicată în „războiul" asigurării Securității Naționale. Așa poate fi și, din păcate, așa este de multe ori abordată problema. Greșită abordare zic alții și... mă număr printre ei.

Cu ce argumente?... ar trebui să vină imediat întrebarea scepticilor sau necunoscătorilor.

Vin prompt cu exemple:

1. pentru că un ziar central publica în anii '90 o știre despre o captură de droguri în portul Constanța, informație „scăpată" probabil de cineva din cercul celor care chiar au lucrat la „rezolvarea" cazului, un al doilea transport de stupefiante a fost scăpat de Interpol, vasul cu pricina ne mai ajungând niciodată în apele teritoriale ale României unde echipele de polițiști din mai multe țări îi pregăteau capturarea. Sute de kilograme de drog au ajuns pe alte piețe, au fost probabil comercializate și au finanțat probabil structurile internaționale teroriste sau cercurile mafiote. Rețeaua de traficanți, care a fost la un pas să fie anihilată, a continuat să-și vadă de treabă din cauza unui „banal" articol de ziar.

2. Martie 1990. Târgu-Mureș, Cofariu. Așa se poate concentra un moment puțin spus delicat din istoria post decembristă a țării. Ziariști străini se aflau acolo înainte ca evenimentele să o ceară, înainte ca „ceva" să fie de filmat sau relatat. Nimeni nu poate spune acum, când tot episodul a intrat și a rămas definitiv între coperțile manualelor, nescrise încă, de istorie că nu a fost vorba de o criză care aducea grave atingeri Securității Naționale. La baza „inițierii" crizei cât și a modului în care a fost gestionată s-a aflat și...presa.

3. Integrarea României în NATO precum și demersurile menite a sprijini integrarea în Uniunea Europeană au o componentă mediatică majoră. Un succes și un deziderat. Două ținte în atingerea cărora presa a jucat și joacă un rol important. În ambele cazuri Securitatea Națională este definiția de la care se pleacă. Fie că este vorba de siguranța economică sau militară a țării, fie că se ia în calcul poziționarea României în viitoarea arhitectură socio-demografică a Europei.

În aceste două cazuri, rolul presei a fost și este important atât prin ceea ce a făcut și face cât și prin ceea ce... nu a făcut și nu face.

Exemplele pot continua dar relevant, în opinia mea, este doar algoritmul acestora. Am în minte imaginile aparent șocante ale debarcării trupelor americane pe o plajă într-un viitor teatru de operațiuni, imagini transmise „live" de CNN. Rememorez imaginile transmise de același canal de televiziune din Irak. Un set de cadre atent „alese" pentru a servi cauzei.

Cauza, în toate aceste cazuri, o reprezintă sub o formă sau alta, interesul național, printr-o extrapolare deloc greșită zic eu, Securitatea Națională. Indiferent despre ce „națională" este vorba.

Și iată cum venim „acasă"!

Acasă unde cauza este uneori clară și servită de presă în modul cel mai firesc și profesionist cu putință.

Acasă unde cei care au o cauză nu reușesc sau... nu vor s-o facă „lizibilă" și pentru cel mai puternic aliat mediatic potențial: presa.

Acasă unde nu există nici o cauză și totuși mass-media reacționează ca și cum ar exista și se substituie atât inițiatorului cât și ei însăși ca agent purtător de mesaj. Aici sunt cele mai grave derapaje, cu efecte greu de estimat sau gestionat. La acest ultim mod de lucru — ușor de regăsit și în alte cazuri de țări aflate în plin proces de tranziție — se înregistrează cele mai mari „pagube colaterale".

Mass-media este parte a mediului informațional. Un adevăr de care țin seama, sau ar trebui s-o facă, toți cei implicați prin lege să asigure Securitatea Națională a României. Gestionarea riscurilor ca și gestionarea crizelor sunt factori esențiali în procesul de asigurare a răspunsului corect la o largă gamă de amenințări cu caracter strategic. Presa a deținut în istorie roluri de primă mărime în completarea infrastructurilor naționale „critice" cu scop defensiv. Astăzi coordonatele au fost atât de mult modificate de realitățile managementului globalizării încât coordonarea eforturilor de acțiune cu cele mediatice sunt mai utile și eficiente ca oricând.

Într-o țară în care o instituție cu serioase atribuții în domeniul Securității Naționale — mă refer aici la Agenția Națională de Control al Exporturilor — nu are nici o structură, când spun nici o structură a se înțelege nici o persoană, abilitată să țină legătura cu mass-media este dificil de realizat o comunicare eficientă între oficialități și cetățean, pe de o parte, și între intern și extern pe de alta.

Efectul primar? Gestionarea incorectă a situației create de o navă care transporta arme importate din România, navă subiect de presă și în țară dar mai ales în presa străină.

Efectul secundar? Deficit de imagine în procesul de armonizare a legislației și măsurilor operative în domeniul controlului de exporturi speciale. Spun de imagine pentru că, în fapt, lucrurile erau clare și din punct de vedere legislativ și procedural.

Unde este vorba de Securitate Națională? Se pot întreba unii.

Acolo unde orice deficit de imagine poate contribui la tergiversări sau noi condiționări în drumul spre Europa.

Plecăm de „acasă" pentru a vedea, în câteva fraze, care sunt vulnerabilitățile presei, oriunde s-ar afla ea în lume, care pot fi cercurile de constrângere și care efectele acestor posibile încorsetări. Fac analiza referitor la presă în general cu precizarea că, acolo unde aceasta operează într-un mediu încă instabil economic și dominat de transformări politico-sociale profunde, labilitatea față de sistem este sporită.

DEPENDENȚA DE POLITIC

Cazurile „Europa Liberă" sau „Vocea Americii" — în ceea ce privește spațiul fostului lagăr comunist (nu doar România era teritoriu țintă) sunt relevante pentru ceea ce înseamnă un canal media în lupta de desființare a „cortinei de fier". La fel poate fi evaluat CNN-ul în anumite cazuri dar cu alte coordonate de impact și bineînțeles alte teritorii țintă. În cel

de-al doilea război mondial posturile pirat de radio au reprezentat unul dintre pilonii de sprijin moral și de coordonare operativă a acțiunilor militare în teritoriile ocupate. Deși părea „presă", act de cultură pe un post de radio, versurile lui Paul Verlaine reprezentau coduri indispensabile rezistenței franceze în acordarea de sprijin logistic și militar aliaților care debarcau în Normandia. Anunțurile publicitare din cotidienele vremii sau articole aparent fără conotații reprezentau în fapt același lucru: mesaje codificate utile luptei de eliberare. Politicul coordona acest mecanism de presă în scop bine definit în fiecare din cazurile de mai sus. În zilele noastre războiul s-a mutat în plan economic, politic sau demografic. Acum politicul dictează tonuri iar abordarea mediatică compune „melodii". Acum se caută câștiguri la masa verde a tratativelor, poziționări cât mai avantajoase în viitoarea arhitectură a „satului" universal sau modificarea zonelor de influență economică. Cât a contribuit mass-media la declanșarea războiului din Irak — de data aceasta cu arme și tot arsenalul militar clasic — într-un context antiterorist mondial? Cât a contribuit presa, mai ales cea audiovizuală, la pornirea luptei antiteroriste la scară planetară după 11 septembrie 2001? Dar după atacul din decembrie 1941 de la Pearl Harbour?

Repet! Este vorba de o dependență a presei de politic în sensul sprijinirii eforturilor de garantare și dezvoltare a Securității Naționale.

DEPENDENȚA DE ECONOMIC

La un curs de deontologie a presei, ținut la Chico State University — California în 1991 de un reputat profesor american, ni se spunea nouă, ziariștilor veniți din țări central și est europene că, citez, „cine dă banul face legea în presă". Greu de digerat și de acceptat pentru cel care eram la acea vreme, reporter în Televiziunea Română ...Liberă... adevărul

însă acela era și aveam să-l înțeleg abia peste ani. De ce? Pentru că la București nu se așezaseră încă lucrurile. Acum este cu totul altceva.

Dar să revenim la... alții.

Marile concerne de presă de pe glob au „în spate", mai mult sau mai puțin, potentați ai sferei economice. În multe cazuri se completează „garda" cu politicieni „de marcă". Exemplele din fostul spațiu sovietic sunt cele mai răsunătoare deși... nu sunt cele mai relevante. Sunt „zgomotoase" pentru că nu s-a așezat încă societatea pe baze stabile. Stabilitatea, în acest context, nu elimină dependența de economic ci doar o face mai suplă, mai liniștită și mai eficientă.

Se poate naște întrebarea: ce legătură au aceste afirmații cu tema propusă. Dacă însă se evaluează corect ce reprezintă economicul în asigurarea Securității Naționale, și un profan îi poate constata importanța majoră. Nu se mai pune problema cuceririi de teritorii cu arma în mână. Este suficient să-ți impui „jocul" comercial și „strategia" economică. În secolul trecut, înaintea unei operații militare de infanterie, artileria făcea pregătirea de înaintare. În secolul XXI infanteria este înlocuită cu „transnaționalele" iar artileria cu un set de măsuri între care „pregătirea mediatică" are un rol important. Este adevărat că nu toți factorii de decizie de aiurea au înțeles și aplică aceste principii de lucru cu efecte deja verificate.

Mai mult! Și în interiorul unei țări, deci în granițele aceleași economii, interesul financiar „mână în luptă" multe trusturi de presă cu la fel de multe „culise" de partid, de grup sau personale. Când acest angrenaj intră în coliziune cu altele, similare ca putere financiară dar opuse ca interese, se poate face mai mult ca sigur și un bilanț al „atingerilor" aduse Securității Naționale căci, inconștient sau nu, „maieul este mai aproape decât cămașa" sau lipsa de perspectivă asupra efectelor colaterale este mai mare decât dorința de a câștiga.

Venim „acasă" din nou!

Care au fost demersurile celor abilitați să gestioneze Securitatea Națională a României în ceea ce privește colaborarea aducătoare de profit sigur cu presa din țară și...nu numai?

Care au fost învățămintele trase din modul în care s-a folosit până acum imensul capital de credibilitate și impactul uriaș la public pe care-l are mass-media? Care sunt măsurile luate pentru ca presa să contribuie eficient la gestionarea crizelor sau managementul riscurilor cu care s-a confruntat și cu siguranță se va confrunta și mai abitir România?

Mi-aduc aminte ce reacție au avut oficialitățile noastre în urmă cu 5 ani în cazul dramatic — dar receptat ca fiind așa de puțină lume — al unei importante Bănci din România. Atacul împotriva respectivei instituții a avut o puternică componentă...mediatică. Printre alte măsuri strict necesare și just puse în practică...s-a apelat și la sprijinul presei. Era nevoie de semnal concertat care să țină banca, din punct de vedere al imaginii „la vedere", la cote de credibilitate pe măsura importanței acesteia. Presa a reacționat prompt dar...cu stângăcia și temerea celui nepregătit pentru astfel de situații. A fost un demers eficient, totul s-a terminat cu bine, presa a fost apreciată. A rămas însă, pentru mine și pentru alți ziariști care au pus umărul, gustul amărui al lipsei unui algoritm de lucru în astfel de situații.

Sunt, sau cel puțin așa știu, foarte puțini ziariști români care înțeleg cum să abordeze o situație specială, care să poată discerne și acționa în consecință în cazuri de eveniment cu „atingere la siguranța națională". Dacă greșesc îmi fac „mea culpa". Dacă nu greșesc...este grav.

Mi-aduc iarăși aminte cum doi ofițeri de rang înalt din armata română se străduiau în 1998 să-mi explice importanța operațiunii „Floare de Colț" la care Prima TV, unde eram director de departament, fusese invitată să-și trimită o echipă de filmare. Era vorba de o acțiune militară cu impact controlat în planul civililor. Se foloseau termeni pe care nu-i cunoșteam în totalitate, se creionau strategii de colaborare pe care nu le înțelegeam în totalitate, se creionau concluzii mediatice și parametrii de verificare a reușitei acestei colaborări pe care... doar în parte puteam să-i văd clar.

Cât de grav este să nu ai, ca țară membră NATO, un sistem de răspuns în acest domeniu? Cât de important este faptul

că la acțiuni importante de sprijin al instituțiilor cu abilitare în domeniul Securității Naționale, la care ar trebui să participe și ziariști — și nu de orice fel — sunt purtători de mesaj mediatic te miri cine?

Dar de ce spun eu „ca membru NATO"?

Oricine vrea să fie cu un pas mai aproape de țintă ar trebui, gândesc eu, să judece cu aceiași măsură cu care judecă cei deja cu experiență în domeniu relația cu mass-media. Poate acum, la finalul cursurilor Colegiului Superior de Siguranță Națională, să am o altă perspectivă a rezolvării acestei importante probleme: relația presei cu...viitorul Securității Naționale.

Spun poate pentru că nu am garanția că se va trece de la utilele cursuri teoretice la o practică atât de necesară României anilor următori. Spun poate pentru că nu știu cum vor fi folosite experiențele altora în folos propriu. Spun poate pentru că eu, personal, sunt limitat în cunoașterea fenomenului și...poate sunt într-o totală eroare. Poate România a rezolvat de mult, corect și eficient problema și eu, în întunericul neștiinței mele, vin aici și bat cu nonșalanță câmpii. Cine știe?

Cert este un lucru!

Astfel de cursuri au o mare utilitate. Lasă cu siguranță ușa deschisă spre o nouă abordare. Nu doar pentru un ziarist, sunt convins. Orice ușă deschisă este, pentru orice om de bun simț, o invitație. Eu am acceptat-o. Este drept că mi-am descoperit alte limite, alte zone de necunoaștere dar...am teme noi. Știu unde am lucrat. Tot este ceva!

Nu știu cât am onorat tema pe care mi-am propus-o dar știu că orice pas mai departe în abordarea ei ar fi fost ori greșit ori periculos.

Cu respect profesorilor CSSN.

MASS-MEDIA ŞI SECURITATEA NAŢIONALĂ

Florin Bruşten

Siguranţa naţională aşa cum este ea definită în legea 51/1991 reprezintă starea de legalitate, echilibru şi stabilitate socială, economică şi politică necesară existenţei şi dezvoltării statului naţional unitar român.

Practic din formularea legii rezultă necesitatea: asigurării existenţei şi dezvoltării statului naţional unitar român; menţinerii ordinii de drept; menţinerii climatului de exercitare a drepturilor şi îndatoririlor cetăţeneşti.

Este evident că la momentul elaborării şi promulgării legii anumite conotaţii istorice au impus utilizarea termenului de siguranţă naţională.

Evoluţia societăţii româneşti post '89, a mentalităţilor precum şi drumul asumat de către ţara noastră în noua configurare internaţională a alianţelor şi a zonelor de interes (post război rece) impun o readaptare a legii 51/1991 în litera, dar poate şi în spiritul ei. Este momentul să nu ne mai ferim în a defini termeni precum securitatea (şi nu siguranţa naţională) precum şi riscurile şi ameninţările la adresa acesteia.

Prin aderarea României la structurile euro-atlantice şi apropiata integrare în Uniunea Europeană, dar totodată şi prin extinderea fenomenului de globalizare au apărut riscuri şi ameninţări noi, alături de cele tradiţionale, la care instituţiile abilitate ale statului trebuie să facă faţă.

Siguranţa naţională devine astfel o parte componentă, dar şi o direcţie de acţiune sau mijloc de realizare a Securităţii Naţionale.

Astăzi nici o ţară nu se mai poate apăra singură. Avem nevoie de o nouă strategie în acest domeniu, integrată procesului de cooperare şi colaborare internaţională (cu componentele sale colectivă, zonală, regională etc.) şi care să corespundă noilor realităţi. Această schimbare strategică impune: eliminarea (protejarea) vulnerabilităţilor; colabo-

rarea internațională intensă și eficientă; schimbarea accentului de pe „reacție" pe prevenție.

Așezarea doctrinei de securitate pe un fundament nou atât din punct de vedere legal cât și structural va conduce desigur și la un management eficient. Este o condiție necesară nu și suficientă însă.

Nu putem gândi la cum vom acționa dacă nu vom ști și spre ce dorim să ne îndreptăm. Cum ar trebui să arate România (privită ca un sistem complex integrat în macrosistemul internațional) peste 5 ani? Dar peste 10 sau 20 de ani? Știm noi acum acest lucru? Eu cred că nu.

Doar așa vom putea aproxima cât mai bine harta mediului de securitate. Vom putea să gândim preventiv, să dimensionăm posibilele abateri, să identificăm soluții de moment sau de etapă și vom ajunge să schimbăm atitudinea reactivă în cea preventivă. La scara istoriei o secundă, o oră, un an au valoare zero. La scară umană însă...Cu tot progresul tehnologic un lucru este sigur: *nu vom putea întoarce niciodată timpul înapoi*, iar îndreptarea greșelilor făcute ne va costa mult mai mult decât ne costă acum prevenirea lor.

DE CE MASS-MEDIA ȘI SECURITATEA NAȚIONALĂ?

Este media o componentă atât de importantă a mediului de securitate? Media înseamnă comunicare, comunicând transmitem informații. Cine deține informațiile și totodată poate interveni în procesul de modelare a acestora poate deveni un actor important al puterii sociale, participând sau chiar fiind motorul în procesele de construire (și/sau combatere) a strategiilor câștigătoare, dar și în cele de control al comportamentelor.

Încheierea războiului rece a presupus o schimbare radicală a modului de evaluare a raportului de forțe și o nouă formă credibilă de descurajare strategică-războiul informațional. El presupune nu numai cunoașterea ci și dominarea prin influențare a mediului informațional din „spațiul inamic", în paralel cu protecția propriului tău mediu informațional.

Această nouă fază (ce presupune evident și înglobarea formelor tradiționale de război) a condus la trecerea de la „Dușmanul te ascultă" la „Dușmanul știe ce gândești" și mai apoi la *„te determină ce să gândești"*.

Are media un rol important în acest război? *Eu cred că da* și în cele ce urmează voi încerca să aduc doar câteva argumente.

Rolul mass-media este de a comunica cu masele prin diverse tehnici de transmisie, în mod indirect (la o distanță spațială, temporală între partenerii de comunicare) și *în sens unic* (de la emițător la receptor)[112].

David Mc Clelland[113] încearcă să identifice corelația dintre perioadele de creștere, respectiv stagnare economică și prezența sau absența unei motivații de performanță în rândurile populației, precum și de relația acestei motivații cu mass-media. Concluzia la care Mc Clelland ajunge este că sarcina primară a construirii performanței este *formarea unor personalități* și nu schimbarea unor structuri sociale tradiționale și deci, implicit îmbunătățirea comunicării (atât în ceea ce privește infrastructura dar și a mas-mediei ca factor de informare și educare).

Daniel Lerner[114] afirmă că tendința de modernizare a unei societăți este strâns legată de consumul de mass-media. Aceste teorii au stat la baza programului UNESCO de îmbunătățire a condițiilor de trai în țările mai puțin dezvoltate prin care trebuiau atinse următoarele cifre: 10 cotidiene, 5 radiouri, două televizoare și două scaune de cinematograf la 100 de locuitori.

Unul dintre cei implicați în acest program, Wilbur Schramm[115] identifica și 11 domenii în care mass-media poate fi de folos într-un proces al dezvoltării naționale: lărgirea orizontului; focusarea atenției; ridicarea nivelului pretențiilor; furnizarea unor contribuții indirecte la schimbarea unor

---

[112] Michael Kunczic și Ashid Zipfel, *Introducere în știința publicisticii și comunicării.*

[113] Mc Clelland, *Societatea de performanță*, 1961.

[114] Daniel Lerner, *Apusul Societății Tradiționale*, 1957.

[115] Wilbur Schramm, *Mass Media și Dezvoltarea Națională*, 1964.

atitudini și disponibilități de acțiune; alimentarea canalelor de comunicare interpersonală cu informații; conferirea unui statut social; extinderea dialogului politic; impunerea unor norme sociale; formarea unor noi „gusturi"; Schimbarea unor atitudini ușor ancorate (cu rădăcini subțiri); Contribuție substanțială în toate domeniile educației.

MASS-MEDIA ÎN PERIOADA COMUNISTĂ

Înainte de 1989, în perioada comunistă mass-media a fost guvernată de așa numita „teorie sovietică a presei"[116]. Sarcina principală a presei era contribuția la păstrarea și propășirea sistemului socialist și al partidului care-l promovează. Mass-media era controlată de către stat și era definită totodată ca braț direct al statului. Principalele deosebiri față de alte sisteme de presă din epocă erau: eliminarea motivației de profit în mass-media; actualitatea devine criteriu secundar în prezentarea știrilor; rol activ în dezvoltarea și schimbarea societății pentru atingerea comunismului.

Dar principala caracteristică a presei în această perioadă a fost manipularea. Treptat, pe măsură ce condițiile de trai se înrăutățeau gradul de credibilitate în mijloacele mass-media interne a început să scadă la un număr din ce în ce mai mare de receptori, producându-se astfel *mutarea centrului de credibilitate* din interior la exterior („Vocea Americii", „Europa Liberă", „BBC", „RFI", „Deutch Welle" etc.). A devenit astfel posibilă (în concordanță desigur și cu schimbările politice din epocă) o influențare din ce în ce mai mare a opiniei publice prin aceste mijloace și implicit de creștere a „temperaturii sociale", favorizând astfel orice fel de acțiune din exterior. Este explicabilă și în acest mod creșterea gradului de acceptare a schimbării, precum și influențarea unor atitudini

[116] Frederick S. Siebert, Wilbur Schramm, Theodore Peterson, *Patru teorii ale presei*, 1956.

în domeniul „acțional". Anul 1989 poate fi considerat unul al experiențelor în ceea ce privește noul tip de confruntare „Războiul informațional" și demonstrează cât de eficientă este o astfel de strategie.

MASS-MEDIA ÎN ROMÂNIA. CONSTRUIREA DEMOCRAȚIEI

Evoluția presei în România în perioada de după decembrie '89 poate fi caracterizată drept cea corespunzătoare unui „liberalism sălbatic". Pare nefiresc poate să caracterizăm evoluția mass-media la fine de secol XX cu o teorie ce și-a trăit apogeul în secolul XIX, dar nu putem neglija condițiile sociale, politice și istorice ale acestei perioade. *Nici o societate nu a mai trecut de la comunism la capitalism*, și disoluția vechii orânduiri (prin intermediul revoluției) a condus la descoperirea *„vestului sălbatic'* la care mulți visaseră.

Peisajul anilor '90 la început? O societate cu legi în construcție, cu instituții (din domeniul securității naționale) timorate, cu pluripartitism politic (uneori infantil), cu o economie în prăbușire liberă, cu granițe de o penetrabilitate îngrijorătoare și cu un flagel al corupției explodând exponențial. În căutarea noului motor social, „banul", nici mass-media nu a făcut opinie separată față de restul societății. Adevărul și doar adevărul, presa câinele de pază al noii democrații, a patra putere în stat, libertatea de expresie (chiar și cea a prostiei) sunt sloganele care au inundat toate canalele media. Însetați după informația de care au fost privați atâta timp, românii (mâncând presă pe pâine) au devenit și politicieni, și justițiari, și economiști, și futurologi, și enumerarea ar putea continua la nesfârșit.

Manipulări grosolane sau elevate, provocări, șantaj, partizanate, răfuieli personale sau de grup, toate purtate în numele adevărului, al unui adevăr al emitenților, diferit în cele mai multe cazuri de cel oferit de realitate. Cât a pierdut

România? Câte din greșeli puteau fi prevăzute? Poate mult mai mult decât ne dăm seama. Nu putem să întoarcem timpul înapoi! Un adevăr pe care, din păcate, uitându-l am plătit, din nou, foarte scump. Măcar de am fi învățat!

Treptat cu greutăți, cu piedici puse din zonele arhicunoscute, cu amenințări și riscuri la care „nici cu gândul nu am gândit" și la care priveam înainte cu nedumerire și detașare (terorism, criminalitate transfrontalieră etc.) tânăra democrație românească a reușit să se închege. Nu întâmplător odată cu aceasta și mass-media și-a schimbat „înfățișarea", din presa liberală încercând să devină una „responsabilă social" și implicată în „dezvoltarea națională".

Câștigul major al revoluției l-a reprezentat însă, pentru presa română, „revenirea în țară" a centrului de credibilitate. O întrebare îmi rămâne însă: Dacă viitorul ne va mai încerca, vreodată, vom mai avea aceiași șansă?

MASS-MEDIA ȘI SECURITATEA NAȚIONALĂ. CONSOLIDAREA DEMOCRAȚIEI

Presa este o componentă importantă a mediului de securitate națională, ea acționând practic în toate subsistemele lui. Dar presa evoluează, și ceea ce credem că stăpânim se dovedește a nu fi suficient. Revoluția tehnologică fundamentală care a generat această nouă societate în care trăim, societatea informațională, a introdus noi necunoscute în ecuația mass-media. Comunicarea a evoluat. Au apărut noile medii. Fenomenul numit generic „multimedia" a mutat destinația comunicării, de la mase la cea individuală de tip „*on demand*", o comunicare la cerere. Folosirea interactivă înseamnă că receptorul devine utilizator, el putând să intervină utilizând diverse canale disponibile, schimbând conținutul și declanșând acțiuni.

Pe lângă aceste provocări componentele „tradiționale" ale mass-media (ziarele, televiziunile și radio-ul) își schimbă

înfățișarea și obiectivele. S-a schimbat deja ponderea și capacitatea de a capta atenția receptorilor pentru a le furniza informații, de la ziare și radio spre televiziuni. Un recent sondaj arată că aproape 80% dintre români se informează de la televizor. Pe de altă parte are loc o trecere, aproape nedetectabilă, de la național spre regional (firească în contextul și cerințele integrării europene), iar sondajele de audiență indică o polarizare accentuată în zona mijloacelor media regionale.

Cine deține controlul strategic al „prelucrării" informației poate să determine și modul în care vom gândi și acționa.

ÎN LOC DE CONCLUZIE

„În societățile complexe — afirma William F. Ogburn[117] — diferitele domenii ale afirmației (familie, drept, educație etc.) se schimbă în ritmuri diferite". Accelerația mai mare este în domeniul tehnico-economic, restul „șchiopătând" după el. Dilema lui Karl R. Propper[118] era că orice dezvoltare viitoare va fi influențată în mod hotărâtor de nivelul tehnologiei viitorului, pe care nu îl putem prevedea. De aceea există în mod pasiv și prognoze și strategii greșite. Dar știm și putem să le readaptăm? Să sperăm că da.

[117] William F. Ogburn, *Social change*, 1922.
[118] Karl R. Propper, *op.cit.*, 1965.

ROLUL PRESEI ÎN APARAREA ŞI ASIGURAREA SECURITĂŢII CULTURALE

Sorana Belciu

„Mass-media **guvernează** cultura, filtrând-o.
Ele valorizează o idee şi devalorizează o alt".

H. Marcuse (1977)

„Ceea ce nu trece prin mijloacele de comunicare în masă, are o influenţă neglijabilă asupra evoluţiei societăţii".

A. Moles (1974)

Pornind de la aceste „vechi", dar deloc „depăşite" afirmaţii, vreau să subliniez rolul important al presei în formarea publicului, în educarea sa vis-a-vis de siguranţa naţională.

Nu trebuie să neglijăm faptul că siguranţa culturală a unei naţiuni este o parte extrem de importantă a sistemului complex de siguranţă naţională.

Practic, cultura şi conştiinţa unui popor dictează liniile directoare ale istoriei, politicii, devenirii sale. În acest context, presei îi revine un rol important, o mare responsabilitate, căci instrumentalizează şi cultura şi conştiinţele, având după părerea mea o dominaţie ideologică.

Dezvoltarea tehnologiilor de comunicare a avut ca efect liberalizarea accesului la produsele media, de unde rezultă şi o creştere semnificativă a consumului mediatic, motiv suficient pentru a ne întreba care este şi care va fi impactul mas-mediei asupra societăţii şi a securităţii sale în ansamblu?!

Industria mass-media nu constituie un simplu aparat care se mulţumeşte să promoveze ideologii. Industria mass-media modelează mentalităţi, creează ideologii. Desigur, unii văd aceasta putere a presei cu ochi buni, alţii sunt sceptici.

Multitudinea de reacţii faţă de relaţia media-democraţie se reduce la două poziţii: una critică, care acuză limitările

impuse de logica mediatică, alta care insistă pe legătura co-substanțială dintre media și deschiderea democratică.

E. Katz (1987) considera că paradigma efectelor limitate este dominantă.

În interiorul ei se manifestă paradigma politică, critică și tehnologică.

Paradigma politică consideră că media ne spun la *ce trebuie* să ne gândim; paradigma critică ne spune la *ce nu trebuie* să ne gândim; paradigma tehnologică — *cum trebuie* să gândim. Recurenta lui *trebuie* indică aluziv ideea puterii presei și a jurnalistului, lider de opinie.

Școala critică (de la Frankfurt) subliniază ideea că sistemul economic și cel politic comandă sistemul media și, deci, controlează societatea.

H. Marcuse afirma că „atunci când mijloacele de informare în masă amestecă arta, politica, filozofia cu reclamele, ele aduc aceste domenii la același numitor-formă de marfă", iar cultura de masă modernă este transformată în mijloc de control psihologic. Într-un cuvânt: *manipulare*.

De fapt, nu cred ca există profesie mai expusă evaluării critice permanente.

În fond, totul se rezumă însă la: receptarea corectă a mesajului media, dar și emiterea de către media a mesajului corect către public.

Informația transmisă corect servește siguranței naționale.

Membri unei societăți dispun de un flux constant de informații: acest flux oferă de exemplu, avertismente privind pericole imediate sau legate de nevoile cotidiene. Indivizii nu sunt chiar atât de manipulați, ei filtreza mesajele, le aleg în funcție de interesele personale, rezultă de aici proba puterii limitate.

Presa nu supraviețuiește decât în măsura în care satisface nevoi și interese. Sunt multiple mijloacele pe care sistemul media le oferă. Or, facultatea de a alege liber înseamnă pluralismul mass-media. Și, prin urmare, nu este atunci media garantul societății democratice?!

MASS-MEDIA ȘI SECURITATEA CULTURALĂ

Problematica atât de importantă a securității culturale este departe de a fi primit interpretarea satisfăcătoare. Ilustrative sunt disputele purtate în plan ideatic referitoare la conținutul conceptului de cultură, patrimoniile culturale, impactul pe care cultura îl are asupra socialului, precum și diferențierile pe care socialul le induce în diferitele culturi. De aceea, putem spune că perioada actuală este marcată de tensiuni între tendința de integrare și cea de afirmare a identităților naționale.

După cum decalajele culturale fac posibile atitudini expansioniste și agresive în condițiile în care decidenții politici estimează eronat consecințele; ei presupun posibilitatea obținerii unor avantaje pe termen scurt, dar nu evaluează și consecințele derivate, succesive pentru zone mai largi, inclusiv pentru omenire și pentru oameni.

Astfel că, din perspectiva deschisă de paradigma procesual-organică, se poate susține că distrugerea unei națiuni, a culturii pe care ea o dezvoltă are consecințe nefaste asupra umanității. Și, după cum arată *„tabloul cultural"* al ultimului sfert de veac, putem susține că scenariile de globalizare prin dezorganizarea statelor, deci a capacității națiunilor de a se gestiona public, induc consecințe derivate ce afectează evoluția culturii umanității.

Iar, pe un alt plan, analizele atestă că agresarea culturală ajunge să fie tot mai periculoasă, întrucât afectează toate culturile, dezorganizează interpretorii sociali, inclusiv pe cei ai agresorilor.

Concluzia este că securitatea națională poate fi afectată de *carențe în evoluția culturii proprii* și de limitele și erorile decidenților politici, dar și de *agresiuni care au ca obiect (ca țintă) cultura națiunii*, îndeosebi acele genuri de manifestări culturale care fac națiunea performantă, capabilă să se protejeze.

În astfel de condiții, pentru a susține sistematic devenirea culturii, pentru a orienta creativitatea spre aspecte de maximum interes social, dar și pentru a dispune de posibilități

de descurajare a unor eventuale agresiuni ce au ca obiect zone din cultura națiunii și de identificare și contracarare a eventualelor agresiuni, este necesară elaborarea unor *strategii de securitate culturală,* în cadrul strategiei naționale de securitate.

SISTEMUL MEDIATIC ÎNTRE TEORIE ȘI REALITATE

Cum arată sistemul mediatic într-o țară democrată? Cum ar trebui presa să promoveze democrația, valorile reale, să-și împlinească misiunea?

Sunt două aspecte importante: presa este responsabilă de rolul libertății exprimării în societatea civilă; relația jurnalism-democrație-securitate într-o epocă de globalizare.

În multe societăți democratice, legea presei și a culturii, ca și cea a libertății expresiei sunt încă perfectibile. Sunt însă multe realități care frânează procesul dezvoltării și cultivării libertății presei. Există tensiuni între dorința de a promova libertatea expresiei și cea de a construi societatea civilă.

Există însă un echilibru? Sunt riscuri sociale și politice de a l-e evita într-o societate deschisă și liberă? Se pun astfel de întrebări chiar și în țările cu o bogată tradiție democratică. Răspunsurile tipice vin însă pe cale legală, constituțională și prin practica jurnalistică și culturală.

Confluența tuturor acestor factori determină balanța libertăților și a responsabilităților sistemului mediei.

BIBLIOGRAFIE

J.B. Thompson, *Media și modernitatea. O teorie socială a mass-media,* ANTET, 1994.

I. Drăgan, *Paradigme ale comunicării de masă,* Șansa, 1996.

J. Habermas, *Sfera publică și transformarea ei structurală,* Univers, 1998.

Cr. Florin Popescu, *O introducere în receptarea mesajului mediatizat,* ANI, 2001.

Marian Petcu, *Sociologia mass-media,* ANI, 2001.

MASS-MEDIA — PRELUNGIREA ACTULUI TERORIST?!

Carmen Crețu

După 11 septembrie 2001 istoria va fi împărțită în două: înainte și după atacul terorist asupra Turnurilor Gemene. Analiști și istorici sunt de acord că nimic numai este ca înainte. Chiar dacă am fost obișnuiți cu atentatele din anii '70 ale Brigăzilor Roșii sau cu războiul dus decenii de-a rândul de către IRA, ca să numai vorbim de atentatele palestiniene din conflictul arabo israelian, 11 septembrie, pe lângă tragedia în sine, a ridicat probleme complexe și a creat o nouă perspectivă legată de conceptul de securitate. După acest atac terorist s-a impus o abordare cu totul și cu totul nouă a celui mai puternic flagel al societății globale direcționată spre dezvoltarea *high-tech*.

Terorismul, în forma sa globalizată, reprezintă acum factorul de risc numărul unu declarat pe plan mondial mai mult sau mai puțin oficial. Odată cu atacul nefast din 11 septembrie au început să se pună o mulțime de întrebări la care nu se prea găsesc răspunsuri viabile. Una dintre dintre acestea este următoarea: *poate fi considerată preluarea și retransmiterea imaginilor dezastrului de către absolut toate canalele de televiziune din lume, ca o prelungire în zilele imediat următoare a atentatului? Faptul că au fost mai apoi propagate imaginile șocante, poate fi socotit ca făcând parte din chiar atacul terorist?*

Fără îndoială, că toate rețelele de televiziune — indirect, pentru că respectau dreptul fundamental al cetățeanului la libera informare — au devenit propagatorii și instrumentul cel mai eficace al lui Osama Ben Laden de a transmite un mesaj de amenințare, un mesaj de teroare. La fel și discursul către lume în care își expunea motivațiile, reluat mereu și analizau până în cele mai mici detalii, era sau nu o formă de terorism? Obținuse atenția mondială și o publicitate la un nivel nemaiîntâlnit până atunci. Cum poate fi neutralizată

o astfel de situație, fără a deveni o societate închisă, totalitară, în care să se încalce dreptul cetățeanului de a fi informat, accesul său la informație?

Experți în mass-media, sociologi, analiști, istorici etc., și-au expus pe larg în zeci de articole și publicații diferite teorii și ipoteze dar până în acest moment concluziile nu par a fi edificatoare.

O dată cu trecerea timpului și efectuarea unor măsurători, mai ales de către cercetătorii din domeniul războiului psihologic, se dovedește că impactul asupra psihicului a milioane de oameni, care au urmărit imaginile cu cei care se aruncau de la etaj, din cauza fumului, din turnurile țintă, a fost la fel de traumatizant încât i-a transformat în victime de război, în masă de manevră pentru un șantaj din partea teroriștilor. S-a declanșat odată cu acele evenimente un gen de război de o violență a terorismului fără precedent. Mass-media s-a dovedit a fi un instrument accesibil teroriștilor tocmai într-o societate democratică, în care principiul dreptului cetățeanului la informație este sacrosant.

Pe măsură ce armele biologice și de distrugere în masă se diversifică și pot fi fabricate mai ușor din cauza accesului la informația tehnologică și la dezvoltarea echipamentelor tehnologice, terorismul a devenit o amenințare mult mai puternică decât s-ar fi crezut, de pildă , în urmă cu cinci ani. Pe lîngă aceasta el capătă forme din ce în ce mai subtile. Însă atacurile teroriste din ultima vreme se bazează pe multe procedee și tehnici folosite în războiul rece. Ca și cum odată cu terminarea acestuia, experiența dobândită de cele două mari puteri aflate în conflict, U.S.A. și URSS, s-ar fi transferat organizațiilor teroriste. Implantarea de agenți în diferite posturi cheie, crearea de rețele (este cunoscut faptul că organizații fundamentaliste islamice plătesc persoane aflate în cele mai diferite puncte ale societății), crearea de campanii de presă, nimic nu scapă celor care organizează și crează crize în cadrul acestui război.

Aplicarea unor tehnici și desfășurarea unor operațiuni ale acestui gen de conflict neconvențional în domeniul cel mai

fluctuant și fragil, cel al mass mediei, face ca odată cu globalizatea informației, să ne aflăm în fața celui mare pericol care a amenințat vreodată civilizația și umanintatea.

Terorismul folosește orice fel de armă: fie că este bacteriologică, convențională, psihologică. De aceea, cele mai afectate sunt societățile democratice. Fiind puse în situația de a-și apăra interesele, de a-și conserva securitatea dar și de a respecta regulile democratice, acestea (fiind și cele mai amenințate) sunt pe cale de a-și edifica regimuri *autoritare* (atenție nu totalitare). Pe de altă parte, ele sunt obligate să ducă campanii de educare a populației pentru a-i crește competența în ceea ce privește interpretarea informațiilor care-i vin prin canalele mass-media. Mass-media este factorul numărul unu în disputa mentalului publicului...

Depinzând aproape în întregime de informație, *homo sapiens* al începutului mileniului III a devenit vulnerabil în primul rând la comunicarea prin informație. Cu o sută de ani în urmă, sau doar cu câteva decenii în urmă, puținele afirmații publice ale unui lider politic sau militar se bucurau de o credibilitate aproape inalienabilă, iar un articol de ziar constituia un reper al adevărului, indiferent de realitate. Astăzi, valurile de declarații sau chiar fluxurile de imagini, multe dintre ele transmise în direct, nu reușesc să mai convingă și să învingă scepticismul generat de prea multe experiențe nefaste. Cu toate acestea, oamenii au nevoie și consumă în cantități din ce în ce mai mari informații de orice fel, din cele mai diferite surse, cărora fiecare le aplică propria grilă de percepție și înțelegere. Conștient sau nu, cetățeanul înghite (adesea pe nemestecate) informații, deoarece a devenit conștient că nu se mai poate supraviețui fără ele, cu toate riscurile pe care acest consum le presupune și care este mai mult sau mai puțin conștient.

Puterea informației a ajuns așa de mare încât reușește să o complementarizeze și uneori chiar să o domine pe cea a armelor. Astăzi, nici o victorie militară, politică sau economică, (acum nici teroristă) nu mai este cu putință fără o susținere și o dominație informațională corespunzătoare. La

mijlocul anilor '90, vicepreședintele american, Al Gore, recunoștea că stăpânirea universului mediatic este vitală pentru marile conglomerate industriale, deoarece *autostrăzile informației* reprezintă pentru Statele Unite de astăzi ceea ce infrastructurile de transport rutier au însemnat la mijlocul secolului al — XX-lea. Adesea, o campanie informațională bine țintită, sprijinită eventual de câteva intervenții militare chirurgicale extrem de discrete și speciale, devine o alternativă mult mai atractivă decât primitiva opțiune a războiului total sau limitat de altădată. Din nefericire, și teroriștii au înțeles acest lucru și ei știu să exploateze, cu o din ce în ce mai mare eficiență, tocmai această nouă vulnerabilitate umană la informație, beneficiind în plus și de atotputernicul argument al eficienței în privința raportului costuri/beneficii (pentru ei).

Nivelul spiritual al civilizației la care a ajuns societatea umană nu mai permite holocausturi și nici alte distrugeri materiale masive. În fața unei agresiuni informaționale (fie aceasta și totală) rafinate și subtile, nimeni nu pare să aibă nici o obiecție, fiind îndeplinite majoritatea criteriilor și exigențelor lumii civilizate, inclusiv a eventualelor obiecții morale. Evoluția ascendent exponențială a armelor informaționale din ultimii ani — și media poate fi încadrată fără rezerve aici — a depășit baza legală internațională care nu a reușit să găsească soluții juridice în dreptul public internațional și în cel al războiului, pentru reglementatea acestui domeniu. Practic nu există în acest moment, în legislația internațională, prevederi care să definească o agresiune informațională în sensul modern al termenului și cu atât mai puțin să o limiteze sau să o incrimineze. Cei mai performanți politicieni contemporani și cele mai perfecționate instituții militare din lume au înțeles această nouă realitate a omenirii și au trecut la dezvoltarea cestui nou concept al războiului informațional care tinde să remodeleze întreaga gândire și practică militară și politică.

Fie că se numește Bush, Putin, Saddam sau Ben Laden orice fost sau actual lider politico-militar sau chiar religios contemporan este perfect conștient că nici un demers politic

sau militar major nu are șanse reale de succes și de valorificare a acestuia, fără o susținere informațională adecvată. Cu alte cuvinte doar superioritatea forțelor armate sau inteligența acțiunii politico-diplomatice nu mai sunt suficiente pentru a obține rezultatul scontat. Este nevoie ca acțiunea politico-militară clasică să fie amplu susținută cu întregul arsenal informațional disponibil, pornind de la relațiile publice, campanile mediatice, de acțiuni psihologiece, de diplomație publică și mergând până la sprijinul informativ al serviciilor secrete, unităților de război electronic, web, etc.

Dr. Jamie Shea, fostul purtător de cuvânt al NATO din perioada conflictului cu Yugoslavia, este de părere că un război nu poate fi câștigat doar prin campanii mediatice (aserțiune demonstrată de evoluțiile din cel de-al doilea război din Golful Persic), dar poate fi pierdut printr-o politică mediatică și de relații publice defectuoase. S-a ajuns până acolo încât, oricât de mult ar irita pe unii butada care spune că nimeni nu-și poate proclama victoria într-un război până când CNN-ul nu confirmă acest lucru, ea exprimă poate cel mai sintetic realitatea informațională a omenirii la începutul mileniului trei.

La 3 februarie 1996, CNN-ul și-a început buletinul de știri cu vestea morții primului militar american din cadrul IFOR, sergentul clasaI, Donald Duran, căruia îi explodase în mâini o mină antipersonal. Sistemul de relații publice al IFOR a permis transmiterea știrii din Balcani la Washington și apoi în întreaga lume în doar câteva ore, sergentul Duran beneficiind de head-line-ul și prima pagină a tuturor marilor instituții de presă din lume, de atenția și onorurile pe care le-ar fi primit doar un general căzut într-un război convențional.

La doar câteva decenii după măcelurile celor două războaie mondiale în care militarii din toate taberele au murit cu sutele de mii, în timpul operațiilor aeriene și speciale ale SUA în Afganistan din octombrie 2001, secretarul de stat al apărării, Donald Rumsfeld, a fost nevoit să dea explicații presei pentru soarta fiecărui soldat american rănit sau ucis în timpul campaniei antiteroriste. Bombasticele și belicoasele comunicate de presă și declarații ale regimului taliban -

difuzate prin intermediul ambasadorului lor în Pakistan și al telviziunii ALK Jazeera — în care erau proclamate distrugeri de elicoptere și avioane americane, ucideri și capturări de militari din forțele speciale, au reprezentat tot atâtea atacuri informaționale (de natură propagandistică și psihologică, camuflate sub umbrella relațiilor publice) a căror țintă a fost special opinia publică din Statele Unite. Ele au trebuit a fi contracarate tot la nivelul la care au fost lansate, adică al celor mai înalte oficialități politico-militare, ajungându-se până acolo încât s-a „raportat" presei faptul că unul dintre americanii răniți în Afganistan avea doar degetul rupt.

Cine stăpânește mintea oamenilor a câștigat pe jumătate războiul!? Încă din 1978, Tuchmann Gaye în lucrarea sa *Making News; A study of Construction of Reality*, a demonstrat vulnerabilitatea spectatorilor pasivi (lipsiți de informație) în fața manipulării prin televiziune. El lansa aici conceptul de ***construcție a realității*** prin programele de știri. Astăzi, este ceva obișnuit ca analiștii politici când expertizează o știre, să ia în calcul, ce agenție o difuzează, ce rețele o preiau și care anume parte din presă o interpretează. Fiecare dintre acești *actanți* sînt identificați ca făcnd parte dintr-o tabără sau alta, dacă este vorba de un conflict deschis, sau în slujba unui grup de interese sau de presiune. De asemenea, sunt atenți la luările de poziție, vis-a- vis de știre, a liderilor politici și a formatorilor de opinie din zonele delicate, dar și la *perspectiva* prezentată de aceștia. Sunt luate în calcul și canalele de difuzare care ignoră evenimentul respectiv.

O astfel de abordare poate fi folositoare în contracararea teorismului prin mass-media. Acum la început de mileniu, globalizarea informației și a controlului asupra ei, competiția tot mai sălbatică dintre corporațiile multinaționale, pun la îndemâna teroriștilor oportunități pentru atingerea obiectivelor lor.

MASS-MEDIA ELECTRONICĂ

Cea mai importantă caracteristică a presei de televiziune este că audiența crede ceea ce vede, de asemenea, este convinsă, că condițiile sociale și judecățile pe care le urmărește pe ecran sunt unanim acceptate și social sancționate, că aceste valori care se degajă, implicit trebuie menținute. O glumă celebră este aceea când un american îl întreabă pe altul în legătură cu un program stupid anost: *De ce m-aș uita la el? Pentru că este la televizor!* — i se răspunde.

Televiziunea creează un profund sentiment al realității, poate și prin imaginile sale fizice, care includ limbajul corpului celor care apar pe ecran, expresiile faciale, intonațiile vocii, ceea ce implică afectivitate. Problema, care se pune, este cine deține postul de televiziune respectiv și care sunt interesele lui.

Interpretarea evenimentelor implică modul în care sunt puse în relație evenimentele, faptele relatate și cauzele lor. Formalizarea unui astfel de context creează opinia în auditoriu, în sensul în care, dacă, jurnalistul trebuie să respecte deontologia profesională, chiar în dauna interesului celui care îl plătește. În realitate mulți jurnaliști de renume sunt actori ai jocului politic, de multe ori investigația jurnalistică ia forma manipulării. Numai este un secret că marile ziare de renume din lume și-au organizat unități speciale de informare, rețele de informatori care le alimentează cu informație de la sursă în timp real. Problema credibilității este cea mai importantă pentru orice operator media. Jurnaliștii practică cel mai adesea, ceea ce în SUA se numește *muckraking*. Este un termen ce desemnează situația în care guvernul este obligat să ia măsuri în urma unei anchete sau a dezvăluirii unor fapte, care țin de partea nevăzută a vieții politice. De multe ori *muckraking*-ul (to muckrake — a grebla gunoiul din grajd) obligă unele departamente ale statului să-și sacrifice proprii oameni, pentru a da satisfacție opiniei publice. În astfel de cazuri, lupta înseamnă un slalom printre drepturile cetățeanului și mecanismele democratice. Organismele investite cu responsabilitatea securității statului trebuie să cunoască

în amănunt procesele legate de mass-media dar și cele care aparțin terorismului pentru a contracara eventualele atacuri.

O altă problemă care se ridică este cea a influențării elitelor. Scriitorii, vedetele, regizorii, artiștii în general au o mare putere de convingere în aparițiile lor publice ; ei sunt folosiți cel mai ades cu complicitatea lor sau nu, în manipularea opiniei publice, în forțarea mâinii decidenților, a acelor factorilor care își asumă politic deciziile.

CINE CONTROLEAZĂ MASS-MEDIA OFICIAL?

Modelul luat în considerare este cel american. Acesta ilustrează cel mai bine modul în care vectorul rezultat în cadrul luptei dintre marile grupuri de interese economice și politice pe de o parte și organizațiile ne-guvernamentale care apără drepturile individuale ale cetățeanului, pe de altă parte, este factorul de echilibru și un *modus vivendi* al democrației americane. Să mai subliniem că democrația americană este unică și nu seamănă cu nici un alt regim din lume, ea fiind de fapt una ce ține de o societate autoritară. SUA sunt considerate la nivelul opiniei generale cel mai democratic stat din lume; asta nu înseamnă că și este în termenii acceptați de standardele europene. După normele experților, SUA este de fapt un stat cu un regim *autoritar*, dar nu *totalitar*. În cadrul acestui regim, guvernul cunoaște și respectă interesele poporului dar și crează mecanisme pentru evitarea atacurilor frontale ale presei împotriva sa. Știrile, în general, difuzate pe canalele media consacrate, alimentează de fapt suportul, sprijinul pentru politicile sale majore, sociale și ideologice.

Aceste valori sunt selectate în funcție de valorile sociale și le regăsim chiar și în cultura de masă de divertisment.

În regimurile ne-autoritare cu o asumare mai largă a libertăților democratice, trebuie să recunoaștem adevărul, guvernele sunt de multe ori slabe și de multe ori corupte, presa are posibilitatea (și chiar o face) să atace guvernul, să stimuleze critica la mai toate politicile majore, iar divertis-

mentul și cultura de masă sunt selectate pe gustul marelui public (chiar dacă asta implică în general practicarea unui divertisment de joasă factură).

Când un ziarist nu mai are credibilitate nu mai are nimic. Există norme judiciare, dar și norme pe care persoanele, care produc programe de știri, nu le încalcă din conștiință profesională. Deși nu trebuie să ne bazăm prea mult pe asta, normele prin care este controlată conduita profesională a reporterilor, redactorilor, editorilor coordonatori, etc., sunt de asemenea standarde morale care țin de credibilitatea lor — cel mai important capital al oricărui ziarist.

Controlul economic este de fapt cel mai eficient. Pe de o parte, în SUA, cel care are destui bani își poate deschide o rețea de televiziune sau un ziar. Cel puțin teoretic. Viața și analiza sociologică, ne învață faptul că mecanismul permite acest lucru numai unui întreprinzător la nivel de corporație... Controlul economic se bazează pe principul *cine plătește hotărăște*. Un ziar care aparține unui proprietar mai sărăcuț este controlat prin publicitate. Această stare de lucruri este cea mai frecventă în statele în curs de dezvoltare și mai ales în cele foste socialiste, care se află la începutul edificării economiei de piață. Pentru a vedea cine îl controlează, este de ajuns să observi, cine cumpără publicitate în cantități semnificative în ziarul respectiv. Poate și de aceea publicațiile și televiziunile guvernamentale sunt considerate într-un fel mai libere de acest tip de control pentru că guvernul le plătește din taxe. Ele nu depind atât de mult de *rating* și de audiență.

În Franța, există o televiziune în serviciu public, France 2, care în mod tradițional este de stânga (indiferent de cine se află la putere); la fel astfel de canale mai există în Israel, Japonia, etc. Controlul asupra unor astfel de instituții se face prin zerourile alocate, la început de an de la buget. Cine trage de mânecă aceste televiziuni? Toată lumea! Și asta pentru că sunt plătite din taxe. Serviciul public este dedicat în general valorilor educaționale și eficiența acestor politici de programe s-a dovedit, în pofida tuturor profețiilor, odată cu succesul canalelor de tip „National Geografic" și „Discovery". Pe de

altă parte, televiziunile din serviciu public sunt cele mai infiltrate de *influențatori* ce aparțin grupurilor de presiune dintr-o societate, pentru că au autoritatea ce decurge din identificarea lor cu administrația care le plătește.

EXISTĂ ÎNSĂ ȘI CONTROLUL PRIVAT ASUPRA MEDIEI?

Bineînțeles că, da! Corporațiile multinaționale își configurează afacerile pe tronsoane imense ale industriilor multiple iar controlul lor asupra unor rețele mass-media este nelimitat. Ele nu pot fi contracarate decât de competitorii lor economici, de legea împotriva monopolului, cât și de faptul că au o credibilitate scăzută, publicul știind că *cine plătește hotărăște* ce se spune și ce nu se spune, cum și în ce context la televiziunea respectivă. Un astfel de exemplu este General Electric. Una dintre cele mai mari corporații mondiale, cu o cifră de afaceri de 60 de miliarde de dolari anual și care deține în active și pasive ca cifră valorică, echivalentul produsului intern brut al unui stat ca Austria. General Electric produce avioane de luptă, motoare de orice fel, sisteme de armament, avionică, echipamente de control, o industrie de producție a plasticelor de înaltă performanță, radare, sonare, rachete, schenere, tomografe cu rezonanță magnetică, echipamente cu ultra sunete, echipamente de menținere a centralelor nucleare, de producție IT, etc. Pe lângă toate acestea ea deține NBC — National Broadcasting Corporation — celebrul NBC cu 200 de stații afiliate pe întreg teritoriu SUA și câteva zeci în afara acestuia. Cine poate ține piept unui astfel de monstru economic? Ce se poate întâmpla dacă în fruntea bordului unei astfel de corporații prin mecanismele economiei de piață ajunge președinte un Osama Bin Laden? Cine îi poate ține piept? Există și un *lobby* al cetățenilor, un control al organizațiilor ne-guvernamentale. Exemplele sunt tot din SUA Cel mai cunoscut și de temut este *National Citizens Committee of Broadcasting* (NCCB); acesta este renumit pentru mili-

tantismul său pentru un control mai puternic asupra mediei de către guvern (pentru a înțelege asta trebuie să înțelegem mai bine ce înseamnă libertatea presei în această țară — unele efecte nefaste le vedem și la noi la „știrile de la ora 5"...) Alte grupuri sunt: *Accuracy in Media* (AIM), un grup conservator ce monitorizează calitatea știrilor și adevărul prezentat în cadrul acestora, *Media Coalition for Better Television* (CBTV), reprezentând forme de apărare ale valorilor tradiționaliste, religioase.

Media mai poate fi controlată și prin manipularea accesului ei la informații. Există informații publice, și aici este o discuție mai largă, și informații clasificate. Mai toate marile ziare sau televiziuni au acces la informațiile clasificate cel puțin la un procent din acestea, în medie cam 10%. În urma unui studiu al lui Dorris Grabber, *Mass media and American Politics*, s-a constat, că oricât de vigilente ar fi organismele responsabile, ele nu pot face față scurgerilor de informații. Procentul minim fiind în jur de 5–6%. Tot ce se poate face este limitarea acestuia, eliminarea fenomenului fiind imposibilă, în societățile care se socotesc democratice.

UNDE SE JOACĂ CONDIȚIONAREA DEMOCRATICĂ A MASS-MEDIEI?

Există o graniță a controlului guvernamental dar și o limită a libertăților celor care fac știrile. Pentru a lămuri și mai bine lucrurile să analizăm puțin statutul editorului coordonator de știri.

În 1974, Patrick Tornillo a dat în judecată un ziar pentru că i-a refuzat dreptul la replică în urma unui articol care i-a produs daune în campania electorală. Ziarul a câștigat. Curtea de Justiție considerând că libertatea editorului ziarului prevalează asupra dreptului la replică a celui incriminat.

Editorul are dreptul nelimitat de a decide ce rămâne și ce nu în paginile ziarului. Regulile nu sunt aceleași pentru media electronică. Cei care deschid o televiziune au nevoie

de o licență și de o frecvență de emisie din partea guvernului. Asta înseamnă că ei depind de acordul pe care trebuie să ți-l dea de a nu încălca anumite reguli impuse de guvern. Printre acestea se află reglementarea prezenței persoanelor politice cu timpi egali... Acest lucru este important pentru că s-a observat că organizațiile teroriste de genul celor fundamentaliste sprijină anumiți candidați la funcții politice, mai ales în țările democratice. Cetățenii au dreptul de a a-și exprima opiniile liber în mass-media. Acest principiu este unul din portițele prin care anumite minorități pot fi manipulate prin nemulțumirile lor în scopul perturbării echilibrului social.

ACCESUL LA DOCUMENTELE GUVERNAMETALE

Documente legate de securitatea națională sunt prohibitive peste tot în lume. Cu toate acestea, informații legate de negocieri, de anumite eșecuri în funcționarea unor echipamente (militare de exemplu) scapă în mod controlat sau nu în mass-media. Aceste scurgeri sunt manipulate după procedurile războiului rece, și ne întrebăm ce se întâmplă când ele ajung pe mâna unei organizații teroriste, care sub pălăria democrației le trimite în zona dezbaterilor publice?

Accesul restricționat se extinde și la anumite informații din documentele unor firme și corporații din industriile și afacerile private. De multe ori stabilitatea economică a acestora ține de securitatea statală.

Tot mai multe guverne puternice și care au un cuvânt de spus prin comunitățile lor de *intelligence* și-au creat o rețea de agenți acoperiți în interiorul canalelor și posturilor internaționale sau naționale de televiziune. În comunitatea *intelligence* este deja cunoscut un fel de *status-quo*, astfel încât fiecare își plasează o persoană în punctele cheie. Se urmărește prezența unui *observator* asupra *acurateței* informației, ajunsă pe canalul de difuzare. Aceștia nu o blochează decât în caz de forță majoră dar *supraveghează* modul în care aceasta pleacă.

O altă formă de manipulare este folosirea procedurilor de selectare a unei știri când se acoperă o actualitate pentru o perioadă scurtă de timp, 24 de ore. Chiar dacă știrile sunt din 4 în 4 sau din 6 în 6 ore, ele de fapt acoperă 24 de ore, materialele fiind reluate.

În ultima vreme cei care construiesc o nouă doctrină de apărare la nivelul statelor NATO țin cont de faptul că organizațiile teroriste au trecut la forme de beligeranță mai sofisticate în care folosesc o combinație de structuri de tip celulă (în care fiecare nu cunoaște decât superiorul strict ierarhic și eventual un subordonat) cu rețele de persoane infiltrate în tot mai multe astfel de colective legate de procesarea și difuzarea informațiilor publice. Foști aliați ai americanilor în războiul rece, lideri din organizații teroriste preiau proceduri folosite atunci, care se bazează pe dorința normală a jurnaliștilor de a obține aprobarea, recunoașterea profesională din partea breslei. Toate aceste criteriile de selecționare a știrilor folosesc terorismului internațional. Ei știu că li se asigură gratis prin ele o publicitate imensă, care face parte chiar din atentatul respectiv.

Jurnalismul manipulativ este o practică pe scară largă. Tehnicile au devenit din ce în ce mai subtile. Cum procedăm în această dispută pentru a nu constata, atunci când este prea târziu, că mintea poporului este la îndemâna unui terorist, care își poate permite să plătească o îngrengătură de rețele cu un număr nelimitat de noduri.

Cum putem identifica și crea o *zonă de securitate* în cadrul mas-mediei *generative* (cea care produce programele de știri) dar și a celei *derivative* aceea care preia știrile și le propagă mai mult timp?

Nu există soluții pentru moment. Scenariile sunt multiple. Toate țările civilizate au proiecte de studiu în acest domeniu; deja unele au preluat în doctrina proprie de securitate unele concluzii la care s-a ajuns până acum, dar singura soluție de moment este educarea populației pentru a putea interpreta cu propria minte ceea ce vede pe canalele mass-media. Este singura soluție dar și aceasta este pe termen scurt. Pe

termen lung, numai un studiu serios, care să îmbine cercetarea cu doctrina militară și cu o anume filozofie, despre ce înseamnă conceptul actual de securitate, poate conduce la rezultate.

BIBLIOGRAFIE

Leo Jeffres, *Mass Media Process and Effects*, 1986;

Walter Gant, *The Diffusion of News about the Attempted Reagan Assassination*, Standfort 1993;

Leonard Thomas, *The Power of Press*, Oxford 1986;

Tuchmann Gaye, *Making News A study of Constructing Reality* New York Free Press, 1986,

Merrill John, *Global Journalism*, Longman 1991;

Chamberlin Bill, *The First Amendament reconsidered*, 1982.

Lichtemberg Judith, *Democracy and the Mass Media*, Cambridge 1990.

Niță Dan, Andreescu Anghel, *Terorismul*, 1998;

Pop Doru, *Mass-media și politica*, 2000;

Mircea Mândru, *Lumea între războiul rece și pacea fierbinte*, 2000;

Călin Hențea, *Propagandă fără frontiere*, 2002.

IV. STANDARDE DE CALITATE ȘI PROTECȚIE

ARMONIZAREA PROCEDURILOR DE SECURITATE INTERNĂ CU STANDARDELE ȘI CERINȚELE NATO

Paul Viorel

Fiecare societate care își proiectează dezvoltarea are nevoie de cunoștințe de la cei cu care cooperează în deciziile politice derivate din necesitatea unor răspsuri sincronizate.

Țara noastră este membră a NATO și are alte obligații și oportunități de securitate. De aceea cunoașterea standardelor NATO este utilă în a lua decizii la obiect în relațiile de cooperare.

Consultanța științifică s-a impus. Astfel de materiale documentare sunt o practică curentă la țările cu vechime în NATO.

Din perspectiva problematicii securității, cunoașterea standardelor de lucru este o cerință imediată pentru a nu pierde timpi pretioși în acțiunile viitoare de cooperare, iar zona de abordat să permită „acoperirea" atât a dinamicii evoluției cât și a standardelor de asigurare a calității în activitățiile desfășurate în țară sau în afara țării în relația cu NATO.

Principiul american este „ceea ce este urgent primează în raport cu ceea ce este important". Pentru noi a devenit urgent cunoașterea standardelor NATO. Scopul imediat este de a marca ce știm și ce se regăsește în standardele NATO. Granița trebuie să fie clară, de unde începem zona pe care să o învățăm în scurt timp.

Ne-am propus să lămurim cel puțin următoarele teme: cum să ne pregătim astăzi pentru cerințele de mâine pe linie de a lucra la standarde NATO; care sunt standardele NATO

pentru asigurarea calității folosite în mai toate domeniile de acțiune.

Propunerile de armonizari ale standardelor NATO (de exemplu standardele AQAP) sunt făcute față de standardul EN ISO 9001 din 2000, care în Romania este aprobat în traducere ca SR EN ISO 9001 din 2001.

NATO este opera oamenilor politici și mai puțin a oamenilor din laboratoare.

Pentru mulți dintre cei care vor citi acest material va fi o surpriză să descopere că știu mai mult despre standardele NATO decât înainte de consultarea lui.

Implementarea standardelor NATO, din familia AQAP, a devenit o necesitate.

Prezentul document este adresat celor care vor să cunoască astăzi relația cu NATO de mâine. Această relație va trebui să fie armonizată cu cerințele de asigurare a calității aplicabile fără restricție în activități militare, de justiție, de poliție, până la servicii industriale și economice.

De la înființare, NATO lucrează în regim de asigurare a calității care își are originea în standardele americane de profil.

NATO îi obligă pe cei cu care încheie contracte să implementeze un regim de asigurare a calității similar celui de la NATO.

Englezii au fost primii care au aplicat standardele NATO în armată și în viața civilă. Au urmat cei din Europa de Vest, care au recunoscut și au implementat standardele NATO. Dar imediat au urmat și țările semnatare ale Tratatului de la Varșovia.

Din standardele NATO s-au născut standardele ISO 9000. Astăzi, standardele ISO 9000 sunt implementate de circa 610 000 de firme din aproape 150 de țări.

Comparând codurile de standarde corespondente de la NATO cu cele de la ISO 9000, conținutul clauzelor și coloanele de lucru, precum și cerințele suplimentare NATO, ajungem ușor la concluzia că diferențele de asigurare a calității sunt foarte puține.

În Europa de vest, practicile NATO de asigurare a calității s-au extins cu rapiditate la nivelul instituțiilor de stat și chiar în unități de poliție sau alte organisme finanțate de stat (exemplu recent: unitatea de politie Phoenix din Anglia).

Când conducerea se implică în asigurarea calității nu sunt greutăți la implementarea standardelor NATO sau ISO 9000.

Adesea în publicațiile interne de asigurarea calității, autorii vin cu cerințe suplimentare din practica NATO pe care le prezintă ca noutăți și care, în fapt, au aproape vârsta NATO.

Producția centralelor nuclearo-electrice a folosit și folosește în continuare standardele NATO care au avut numele de AQ 400 prin anii 1980 (AQ este abrevierea de la asigurarea calității în limba franceză), deci România — pe plan tehnic — are deja experiență în aplicarea multor cerințe NATO.

În acest material documentar este prezentată granișa lui ISO 9001 și când trecem în terenul exclusiv al standardelor NATO.

În capitolul 5 sunt detalii la nivel de clauză.

Fiecare clauză NATO este scrisă în clar.

Au fost armonizate tabelele pentru o eventuală utilizare calificată de către cei care lucrează în sistemul de asigurarea calității după standardul românesc SR EN ISO 9001.

Cei care lucrează în regim de asigurare a calității după SR EN ISO 9001 din 2001 vor întelege că: în fapt lucrează după standardele NATO; nu mai este mult până la următoarea stație, când vor fi îndeplinite toate cerințele NATO în asigurarea calității.

Standardul ISO 9001 este apropiat standardelor NATO din familia AQAP. Concluzia rezultată din analiza comparativă între acestea are menirea de a încuraja, fără îndoială, pe cei care urmăresc să facă saltul de la standardul ISO 9001 la standardele NATO. Credem că acestea interesează pe cei care lucrează în principal în armată, justiție, poliție, activități de administrație de stat pentru servicii de control. În ansamblu nu sunt limitări.

De asemenea, se reține că în standardele NATO, cunoscute sub denumirea AQAP-uri, toate cerințele sunt obliga-

torii, pe când în standardul ISO 9001 cerințele sunt parțial obligatorii (cele care dau neconformități majore) și o altă parte sunt cerințe facultative.

În continuare sunt prezentate informații despre asigurarea calității la NATO și modul cum acestea sunt armonizate în practica tehnică, economică și comercială din armată, justiție, poliție până la activități diverse

Pentru cel care cunoaște standardul SR EN ISO 9001 din 2001 și dorește să cunoască standardele NATO va trebui să mai învețe câteva cerințe care sunt prezentate în capitolul 6.

Facem completarea ca la standardele NATO de asigurarea calității (AQAP) avem experiența în economie în ultimii 25 de ani.

Sunt prezentate aplicațiile de armonizare dintre standardele NATO și standardele românești.

A fost luat ca referință standardul SR EN ISO 9001: 2001 care în continuare va fi menționat ca ISO 9001.

Standardul românesc SR EN ISO 9001, care este un standard armonizat cu standardele NATO (de exemplu standardele AQAP), nu este obligatoriu dar în relația cu NATO, fără acest standard, NATO nu acceptă cooperările.

Prevederile din standardele NATO, care trebuie să fie armonizate suplimentar de prestatorii de servicii sau furnizorii de produse sunt prezentate separat, în capitolul nr. „6".

Furnizorul de echipamente sau servicii trebuie să stabilească, să documenteze, să implementeze, să evalueze și să îmbunătățească un sistem efectiv și economic în conformitate cu documentele NATO care includ cerințele din ISO 9001 ca necesare pentru a fi satisfăcute cerințele contractuale.

În țările din NATO reprezentanții guvernamentali pot aduce modificări la cerințele politicii de asigurarea calității.

În țara noastră, în acest domeniu, există experiența în mare parte la multe unități economice.

Aceasta este o certitudine până la nivelul standardului internațional ISO 9001 din 2000, care a fost tradus și acceptat în totalitate ca standard național SR EN ISO 9001 din 2001 și care conține o mare parte din cerințele standardelor NATO-AQAP.

Firmele care au implementat ISO 9001 din timp vor fi găsite pregătite la o eventuală cerere de a proba că au implementat standardele NATO — AQAP.

Pentru unitățile economice care au implementat standardul SR EN ISO 9001 din 2001 este mult usurata munca de a implementa in totalitate standardele NATO din familia AQAP.

Efortul suplimentar pentru a implementa 100% standardul AQAP (NATO) se reduce pentru unitățile economice (care au deja implementat SR EN ISO 9001) la implementarea câtorva cerințe suplimentare, adică cerințele din sectiunea 9 din standardele AQAP.

Pentru armonizarea NATO, cerințele sunt stabilite, documentate, aplicate, menținute, evaluate, îmbunătățite și/sau evaluate, în mare parte, în unitățile economice din țara noastră, care au implementat SR EN ISO 9001.

Pentru un candidat la o recunoastere NATO pentru a primi comenzi, efortul suplimentar al acestui candidat este de a implementa și cerințele de la clauza 9 din standardele AQAP.

Modelarea cadrului institutional românesc este o posibilă soluție care: este o noua identitate a cadrului legislativ.

În conformitate cu cadrul legislativ existent (de exemplu Legea 39 din 1990 și Legea 415 din 2001), Consiliul Suprem de Aparare al Țării este abilitat să gestioneze unitar problemele securității naționale, sub multiplele ei fațete.

Furnizorul de produse sau servicii trebuie să stabilească, să documenteze, să implementeze, să evalueze și să îmbunătățească un sistem efectiv și economic în conformitate cu documentele NATO. Acest document va include cerințele din ISO 9001 plus alte cerințe care se regăsesc în secțiunea nr. 9 din standardele AQAP.

În practica NATO, reprezentanții guvernamentali de asigurarea calității pot aduce modificări la cerințele politicii de asigurarea calității.

Clauzele NATO care nu se regăsesc în cerințele standardului românesc sunt: Clauza 7.7. „Configurarea Managementului"; Clauza 7.7.2. „Planul de Management de Configurare

(CMP)"; Clauza 7.8. „Anduranța și Mentenabilitatea (R&M)"; Clauza 7.8.1. „Sistemul de Anduranță și Mentenabilitate"; Clauaza 9.1. „Acces la furnizor și sub-furnizor precum și suport pentru activitățile lui GQA; Clauza 9.1.1. „Furnizorul și sub-furnizorul vor permite să aibă acces GGQAR și /sau furnizorul intermediar: — dreptul de a avea acces la dotări ori de câte ori părți/ repere de la contract sunt procesate și informații pertinente despre îndeplinirea cerințelor din contract.

Deci avem șase cerințe în plus față de ceea ce se cere în standardul românesc SR EN ISO 9001 din 2001 pentru a îndeplini cerințele NATO. Standardul românesc se poate aplica în toate domeniile de activitate, începând cu justiția, armata până la prestatorii de servicii. Un mic efort în plus și se trece și de aceaste cerințe pentru a fi cu sarcinile NATO îndeplinite.

Extinderea NATO a însemnat și acceptarea țării noastre ca membru cu drepturi depline. Astazi, NATO este și în România. Conferința NATO din iulie 1990, de la Londra, a constituit momentul demarării dialogului cu statele care au aparținut Tratatului de la Varșovia.

În consecință, doctrina NATO — definită ca „apărare înaintată" — a fost supusă unui proces de remodelare conceptuală, fiind în cele din urmă agreată. După 1991, NATO a trecut la evaluarea noii realități.

Evenimentele de la 11 septembrie 2001 se dovedesc providențiale întrucât a fost identificat noul inamic: terorismul internațional. Astazi există tendința tot mai evidentă la Bonn și Paris să se pună capăt dominației SUA.

Elaborarea unei strategii de securitate a României presupune investigații pentru a evalua consecințele intrării în NATO. Astazi obiectivul îl constituie accesul real și egal la resursele de securitate. Apreciem că stabilitatea și echilibrul european nu pot exclude Rusia.

Pentru România s-a încheiat lunga și obositoarea așteptare a intrării *de iure* în NATO și a început un nou drum, de implementare a sarcinilor din aderarea *de facto* la NATO.

De interes pentru securitatea națională a României pot fi reținute următoarele date și raționamente.

Bugetul apărării din anul 2002 al SUA s-a ridicat la 377 miliarde de dolari, aproape egal cu totalul cheltuielilor militare ale restului lumii. În acest ritm, SUA va avea în 2007 impresionanta sumă de 450 miliarde de dolari. Decidenții politici de la Washington au înțeles că influența SUA în Europa s-ar diminua dramatic dacă NATO ar înceta să mai existe.

Din aceste motive Alianța s-a angajat pe drumul dificil al adaptării, al reformelor. Un rezultat vizibil al acestui dificil proces îl constituie diminuarea unității de gândire și acțiune în cadrul mediilor Nord-Atlantice.

Spre deosebire de SUA, țările europene nu-și propun să se constituie într-o putere militară de nivel global, cu capabilități de proiecție a acesteia în orice punct al pământului.

Noul concept strategic avansat de expertii Alianței, care permite ca NATO să lanseze operațiuni militare și în afara zonei de responsabilitate, se dovedește o piatră de încercare, ddar și o decizie de o dimensiune aproape insurmontabilă.

Invitația SUA adresată membrilor NATO de a mări alocările bugetare pentru apărare, în vederea reducerii decalajului tehnologic militar existent, a generat un neașteptat efect contrar. Europenii și-au redus nu doar bugetele pentru apărare ci și efectivele militare, în proporție de 25% până la 50%.

S-a conturat o soluție pur europeană. Uniunea Europeană este cea mai importantă entitate economică a lumii, cu însemne și monedă unică. Pe acest considerent a decis să se impună pentru gestionarea securității continentale.

În Europa se dorește să se configureze o arhitectură proprie de securitate. Această decizie a generat, ca reacție strategică a Washingtonului, lărgirea NATO.

România în mod cert este furnizoare de securitate în Europa și deține atuurile care-i conferă dreptul de a se considera furnizoare de securitate.

Atacurile teroriste de la 11 septembrie 2001 din SUA au constituit un moment cheie al destinului Alianței. Atacurile teroriste au dovedit „fragilitatea forței" și necesitatea redefi-

nirii mediului de securitate internațional. Cruciada declanșată de SUA împotriva terorismului global a pus Alianța în fața unor noi dileme.

Unele state membre ale NATO privesc cu un „optimism rezervat" succesul acțiunilor de export de securitate, întreprinse până în prezent, în Afganistan și Irak.

Un candidat la o recunoaștere NATO, pentru a primi comenzi de materiale militare, producătorul face efortul suplimentar, față de ISO 9001, de a implementa și cerințele de la clauza nr. 9 din standardele AQAP. Aceasta este situația pentru o firmă care implementează standardul românesc SR EN ISO 9001 din 2001.

Cerințele NATO, și aici ne referim la familia de standarde AQAP, secțiunile 4, 5, 6, 7 și 8 , pot fi îndeplinite în scurt timp în mod cert de către firmele care au implementat standardul SR EN ISO 9001 din 2001. Standardele NATO–AQAP au câteva cerințe suplimentare care nu se regăsesc în standardul românesc SR EN ISO 9001 din 2001.

De reținut că, adesea, la implementarea lui ISO 9001 sunt abordate și cerințe suplimentare care, în fapt, sunt din categoria cerințelor suplimentare pentru standardele AQAP. Acest aspect este un argument solid care susține că pentru unitățile economice, unde sunt implementate cerințele din standardul SR EN ISO 9001, nu sunt greutăți în a fi certificați în conformitate cu standardele AQAP — NATO. Mulți care lucrează și respectă SR EN ISO 9001 nu știu că în fapt „respectă" o parte foarte mare din cerințele NATO.

Implicarea NATO în „cruciada" împotriva terorismului internațional, o găsește nepregătită să susțină acțiuni militare împotriva unui inamic indefinit, fără locuri geografice sau apartenență statală și fără obiective care pot fi atacate și neutralizate.

În această etapă a luptei împotriva terorismului nonstatal, țara noastră se află în lupta alături de forțele aliate cu SUA, iar în calitate de membru NATO își îndeplinește îndatoririle care îi revin.

MANAGEMENTUL INFORMAȚIILOR CLASIFICATE — STANDARDE NATO

Valentina Lungu

Accesul la informație este un principiu fundamental al funcționării statului democratic. Fiecare cetățean are dreptul de a se implica în procesele de decizie ale comunității, dar în egală măsură trebuie să conștientizeze că promovarea intereselor legitime ale acesteia presupune și protecția informațiilor clasificate.

Activitatea de protecție a informațiilor clasificate este reglementată prin acte normative specifice, respectiv: „Legea privind siguranța națională a României" (Legea nr. 51/1991), „Legea privind protecția informațiilor clasificate" (Legea nr. 182/2002), „Hotărârea de Guvern pentru aprobarea Normelor privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România" (HG nr. 353/2002), Hotărârea privind înființarea, organizarea și funcționarea Agenției de Acreditare de Securitate, Agenției de Securitate pentru Informatică și Comunicații și Agenției pentru Distribuirea Materialului Criptografic (HG nr. 354/2002), „Hotărârea privind protecția informațiilor secrete de serviciu (HG nr.781/2002), „Hotărârea Guvernului pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România" (HG nr.585/2002) și OUG nr.153/2002 privind organizarea și funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat (ORNISS), aprobată prin Legea nr.101/2003.

CE SUNT INFORMAȚIILE CLASIFICATE?

Informațiile reprezintă orice documente, date, obiecte sau activități, indiferent de suport, formă, mod de exprimare sau de punere în circulație.

Informațiile clasificate sunt informațiile, datele, documentele de interes pentru securitatea națională, care, datorită nivelurilor de importanță și consecințelor care s-ar produce

ca urmare a dezvăluirii sau diseminării ne-autorizate, trebuie să fie protejate, atribuindu-li-se în acest scop o clasificare de securitate. Clasele de secretizare se împart în secrete de stat și secrete de serviciu.

Nivelurile de secretizare se atribuie informațiilor clasificate din clasa secrete de stat și sunt: *strict secret de importanță deosebită* — informațiile a căror divulgare ne-autorizată este de natură să producă daune de o gravitate excepțională securității naționale; *strict secrete* — informațiile a căror divulgare ne-autorizată este de natură să producă daune grave securității naționale; *secrete* — informațiile a căror divulgare ne-autorizată este de natură să producă daune securității naționale.

Informațiile secrete de stat reprezintă informațiile care privesc securitatea națională, prin a căror divulgare se pot prejudicia siguranța națională și apărarea țării.

Potrivit legii, în categoria informațiilor secrete de stat sunt cuprinse, pe niveluri de secretizare, informațiile care se referă la:

a) sistemul de apărare a țării și elementele de bază ale acestuia, operațiile militare, tehnologiile de fabricație, caracteristicile armamentului și tehnicii de luptă utilizate exculsiv în cadrul elementelor sistemului național de apărare;

b) planurile, precum și dispozitivele militare, efectivele și misiunile forțelor angajate;

c) cifrul de stat și alte elemente criptologice stabilite de autoritățile publice competente, precum și activitățile în legătură cu realizarea și folosirea acestora;

d) organizarea sistemelor de protecție și apărare a obiectivelor, sectoarelor și rețelelor de calculatoare speciale și militare, inclusiv mecanismelor de securitate a acestora;

e) datele, schemele și programele referitoare la sistemele de comunicații și la rețelele de calculatoare speciale și militare, inclusiv la mecanismele de securitate ale acestora;

f) activitatea de informații desfășurată de autoritățile publice stabilite prin lege pentru apărarea țării și siguranța națională;

g) mijloacele, metodele, tehnica și echipamentul de lucru, precum și sursele de informații specifice, folosite de autoritățile publice care desfășoară activitate de informații;

h) hărțile, planurile topografice, termogramele și înregistrările aeriene de orice tip, pe care sunt reprezentate elemente de conținut sau obiective clasificate secrete de stat;

i) studiile, prospecțiunile geologice și determinările gravimetrice cu densitate mai mare de un punct pe kilometru pătrat, prin care se evaluează rezervele naționale de metale și minereuri rare, prețioase, disperse și radioactive, precum și datele și informațiile referitoare la rezervele materiale, care sunt în competența Administrației Naționale a Rezervelor de Stat;

j) sistemele și planurile de alimentare cu energie electrică, energie termică, apă și alți agenți necesari funcționării obiectivelor clasificate secrete de stat;

k) activitățile științifice, tehnologice sau economice si investițiile care au legătură cu siguranța națională ori cu apărarea națională sau prezintă importanță deosebită pentru interesele economice și tehnico-științifice ale României;

l) cercetările științifice în domeniul tehnologiilor nucleare, în afara celor fundamentale, precum și programele pentru protecția și securitatea materialelor și a instalațiilor nucleare;

m) emiterea, imprimarea bancnotelor și baterea monedelor metalice, machetele emisiunilor monetare ale Băncii Naționale a României și elementele de siguranță ale însemnelor monetare pentru depistarea falsurilor, ne-destinate publicității, precum și imprimarea și tipărirea hârtiilor de valoare de natura titlurilor de stat, a bonurilor de tezaur și a obligațiilor de stat;

n) relațiile și activitățile externe ale statului român, care, potrivit legii, nu sunt destinate publicității, precum și informațiile altor state sau organizații internaționale, față de care, prin tratate ori înțelegeri internaționale, statul român și-a asumat obligația de protecție.

Legea interzice clasificarea ca secrete de stat a informațiilor, datelor sau documentelor în scopul ascunderii încălcărilor legii, erorilor administrative, limitării accesului la informațiile de interes public, restrângerii ilegale a exer-

cițiului unor drepturi ale vreunei persoane sau lezării altor interese legitime.

Informațiile secrete de serviciu sunt informațiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat.

Informațiile secrete de serviciu se referă la acele activități care, fără a constitui, în înțelesul legii, secrete de stat, nu trebuie cunoscute decât pentru îndeplinirea atribuțiilor de serviciu, divulgarea lor putând prejudicia interesul instituției.

Conducătorii persoanelor juridice de drept public sau privat sunt abilitați să stabilească informațiile care constituie secrete de serviciu, precum și regulile de protecție a acestora și, totodată, să coordoneze și să controleze măsurile privitoare la protecția acestora, în conformitate cu normele stabilite prin Hotărâre a Guvernului.

Legea interzice clasificarea ca secrete de serviciu a informațiilor care, prin natura sau conținutul lor, sunt destinate să asigure informarea cetățenilor asupra unor probleme de interes public sau personal, respectiv a celor de natură să favorizeze ori să acopere eludarea legii sau obstrucționarea justiției.

Principalele obiective ale protecției informațiilor clasificate sunt: protejarea informațiilor clasificate împotriva acțiunilor de spionaj, compromitere sau acces ne-autorizat, alterării sau modificării conținutului acestora, precum și împotriva sabotajelor ori distrugerilor ne-autorizate; realizarea securității sistemelor informatice și de transmitere a informațiilor clasificate.

Măsurile de securitate națională, cât și cele care fac obiectul tratatelor, înțelegerilor și acordurilor bilaterale sau multilaterale la care România este parte, sunt destinate: să prevină accesul ne-autorizat la informațiile clasificate; să identifice împrejurările, precum și persoanele care, prin acțiunile lor, pot pune în pericol securitatea informațiilor clasificate; să garanteze că informațiile clasificate sunt distribuite exclusiv persoanelor îndreptățite, potrivit legii, să le cunoască; să asigure protecția fizică a informațiilor, precum și a personalului necesar protecției informațiilor clasificate.

MODALITĂŢILE DE PROTECŢIE A INFORMAŢIILOR CLASIFICATE

Protecţia informaţiilor clasificate vizează: protecţia juridică; protecţia prin măsuri procedurale; protecţia fizică; protecţia personalului care are acces la informaţiile clasificate ori este desemnat să asigure securitatea acestora; protecţia surselor generatoare de informaţii.

Protecţia juridică constă în ansamblul normelor constituţionale şi al celorlalte dispoziţii legale în vigoare, care reglementează protejarea informaţiilor clasificate.

Protecţia prin măsuri procedurale reprezintă ansamblul reglementărilor prin care emitenţii şi deţinătorii de informaţii clasificate stabilesc măsurile interne de lucru şi de ordine interioară destinate realizării protecţiei informaţiilor.

Toate unităţile care deţin informaţii secrete de stat trebuie să stabilească norme interne de lucru şi de ordine interioară destinate protecţiei acestor informaţii, potrivit actelor normative în vigoare.

Măsurile procedurale de protecţie a informaţiilor secrete de stat vor fi integrate în programul de prevenire a scurgerii de informaţii clasificate, care va fi prezentat, spre avizare, autorităţii abilitate să coordoneze activitatea şi să controleze măsurile privitoare la protecţia informaţiilor clasificate.

Protecţia fizică reprezintă ansamblul activităţilor de pază, securitate şi apărare, prin măsuri şi dispozitive de control fizic şi prin mijloace tehnice, a locurilor în care sunt gestionate informaţii clasificate.

Măsurile de protecţie fizică se concretizează în sisteme automate pentru supraveghere, control, acces, gratii la ferestre, încuietori la uşi, pază la intrări, patrule de securitate, dispozitive de alarmă, mijloace pentru detectarea observării, ascultării sau interceptării, dimensionate în raport cu: nivelul de secretizare a informaţiilor, volumul şi localizarea acestora; tipul containerelor (fişete, seifuri, dulapuri) în care sunt depozitate informaţiile; caracteristicile clădirii şi zonei de amplasare.

Protecția personalului care are acces la informații clasificate și este desemnat să asigure securitatea acestora constă în ansamblul verificărilor și măsurilor de educație protectivă și se realizează prin: verificarea persoanelor în vederea eliberării certificatului/autorizației de acces la informații clasificate; identificarea surselor de fisc și prevenirea incidentelor de securitate care pot conduce la compromiterea informațiilor clasificate; includerea persoanelor într-un sistem permanent de pregătire, în vederea însușirii corecte de către acestea a standardelor de securitate și a modului de implementare eficientă a măsurilor de protecție informațiilor clasificate.

Protecția surselor generatoare de informații (INFOSEC) este ansamblul măsurilor și structurilor destinate protecției informațiilor clasificate prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicații și al altor sisteme electronice, împotriva oricăror acțiuni care pot aduce atingere confidențialității, integrității, disponibilității și autenticității acestora.

Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum și depistarea și prevenirea amenințărilor la care sunt expuse informațiile și sistemele.

PROTECȚIA INFORMAȚIILOR NATO

În calitate de candidată la aderare și țară parteneră în Consiliul de Cooperare Nord-Atlantic (Parteneriatul pentru Pace), România a semnat în 08.07.1994 Acordul de Securitate cu NATO, iar în 10.09.1994 Codul de Conduita și Acordul de Securitate.

Prin semnarea documentelor menționate mai sus, România și-a luat angajamente clare de a „proteja și apăra informațiile și materialele clasificate" ale Alianței și membrilor acesteia, în conformitate cu documentul „Securitatea în cadrul NATO C-M (55) 15 Final înlocuit pentru prima dată de la constituirea Alianței, în anul 2002, de „Securitatea în cadrul NATO — CM (2002) 49 și de Măsurile de Protecție a

Organismelor Militare și Civile NATO împotriva amenințărilor teroriste CM (2002) 50".

NATO, prin instituția sa specializată, Biroul de Securitate NATO (NOS), stabilește standarde de securitate pe care fiecare țară în parte și le adaptează la condițiile proprii.

ORNISS a fost abilitat să asigure implementarea unitară, în domeniul militar și civil, a măsurilor de securitate a informațiilor clasificate, precum și a celor echivalente care fac obiectul tratatelor, înțelegerilor și acordurilor bilaterale sau multilaterale la care România este parte și să exercite atribuții de reglementare, autorizare, evidență și control, în conformitate cu prevederile legii privind protecția informațiilor clasificate, standardele naționale de protecție a informațiilor clasificate și Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România.

Informațiile clasificate NATO se referă la toate informațiile clasificate de natură politică, militară și economică, vehiculate în cadrul NATO, elaborate în cadrul structurilor NATO sau primite de la statele membre ori de la alte organizații internaționale.

Securitatea documentelor clasificate NATO reprezintă ansamblul procedurilor, instrucțiunilor și măsurilor privind gestionarea și controlul acestora (documentul clasificat NATO reprezintă orice document care conține informații clasificate NATO).

Document semnifică toate tipurile de medii de stocare a informațiilor, cum ar fi: documentele pe suport de hârtie, mediile de stocare ale calculatoarelor, microfilme, riboane de printare, dispozitive de procesare portabile.

Prin gestionarea informațiilor clasificate NATO se înțelege totalitatea activităților de primire, de evidență a elaborării și consultării, verificare, evidență, distribuție, transmitere, transport, multiplicare, distrugere, inventariere și arhivare a informațiilor clasificate NATO.

Controlul informațiilor clasificate NATO reprezintă totalitatea activităților de verificare a modului în care sunt gestionate documentele clasificate NATO.

Unul dintre obiectivele importante ale procesului de pregătire a aderării României la NATO constă în asigurarea măsurilor de protecție a informațiilor clasificate (secrete) conform principiilor și standardelor de securitate ale Alianței. În acest sens, un sistem pentru protecția acestor informații trebuie să se bazeze pe măsuri corespunzătoare, specifice securității personalului, documentelor, securității fizice, industriale și INFOSEC, care să asigure un grad comun de protecție a informațiilor clasificate în cadrul NATO.

La baza întregii activități în domeniul protecției informațiilor clasificate se află *principiul „need to know"* (nevoia de a ști) a cărui implementare este necesară în toate domeniile de securitate și mediile de diseminare a informațiilor clasificate.

„Nevoia de a ști" reprezintă stabilirea de către un deținător autorizat de informații clasificate sau sensibile a faptului că o altă persoană verificată corespunzător trebuie să aibă acces la acele informații strict necesare în îndeplinirea atribuțiilor sale oficiale. Prin definiție, principiul este conceput pentru a limita difuzarea informațiilor clasificate, cu scopul de a reduce riscurile de compromitere. El reprezintă o *măsură de securitate solidă*, menită să împiedice divulgarea neautorizată de informații clasificate sau sensibile.

Fiecare utilizator are obligația de a proteja informațiile clasificate care îi sunt încredințate. În acest scop, stabilirea „nevoii de a ști" trebuie făcută de fiecare dată când documentele sunt transmise de la o persoană la alta.

ACCESUL LA INFORMAȚIILE CLASIFICATE NATO. CERTIFICATUL DE SECURITATE ȘI AUTORIZAȚIA DE ACCES

Accesul la informații clasificate NATO se acordă în baza *certificatului de securitate* eliberat de autoritățile abilitate și a respectării *principiului „nevoii de a ști"*.

În cazul în care o persoană deține certificat de securitate sau autorizație de acces la informații naționale clasificate, acesteia i se poate elibera și *certificat de securitate pentru*

acces la informaţii NATO clasificate valabil pentru acelaşi nivel de secretizare sau pentru un nivel inferior. Dacă informaţiile NATO clasificate la care se solicită acces sunt de nivel superior celui pentru care persoana în cauză deţine certificat de securitate sau autorizaţie de acces se vor efectua verificările necesare, potrivit standardelor în vigoare.

În cazuri excepţionale, determinate de situaţii de criză, calamităţi sau evenimente imprevizibile, conducătorul unităţii poate acorda *acces temporar la informaţii clasificate* anumitor persoane care nu deţin certificat de securitate sau autorizaţie de acces, cu condiţia asigurării unui sistem corespunzător de evidenţă.

Certificatul de securitate reprezintă documentul eliberat persoanei cu atribuţii nemijlocite în domeniul protecţiei informaţiilor clasificate, respectiv funcţionarului de securitate sau salariatului din structura de securitate, care atestă verificarea şi acreditarea de a deţine, de a avea acces şi de a lucra cu informaţii clasificate de un anumit nivel de secretizare.

Autorizaţia de acces la informaţii clasificate este documentul eliberat cu avizul instituţiilor abilitate, de conducătorul persoanei juridice deţinătoare de astfel de informaţii, prin care se confirmă că, în exercitarea atribuţiilor profesionale, posesorul acestuia poate avea acces la informaţii secrete de stat de un anumit nivel de secretizare.

Certificatul de securitate, respectiv, autorizaţia de acces se eliberează numai în baza avizelor acordate de autoritatea desemnată de securitate în urma verificărilor efectuate asupra persoanei în cauză, cu acordul scris al acesteia.

Verificările de securitate pentru avizarea eliberării certificatelor de securitate/autorizaţiilor de acces la informaţii secrete au în vedere, conform HG 353/2002 privind „Standardele de protecţie a informaţiilor NATO clasificate în România" şi HG 585/2002 privind „Standardele naţionale de protecţie a informaţiilor clasificate în România", în corelaţie cu standardele de protecţie a informaţiilor clasificate operabile în Alianţa Nord-Atlantică, persoanele care:

a) în exercitarea atribuţiilor profesionale lucrează cu date şi informaţii de nivel secret;

b) fac parte din personalul de execuție sau administrativ și, în virtutea acestui fapt, pot intra în contact cu date și informații de acest nivel;

c) este de presupus că vor lucra cu date și informații de nivel secret, datorită funcțiilor pe care le dețin;

d) se presupune că nu pot avansa profesional în funcție, dacă nu au acces la astfel de informații.

Nivelul de acces acordat prin certificatul de securitate eliberat trebuie să fie similar cu nivelul de clasificare a informațiilor la care persoana necesită acces în îndeplinirea sarcinilor sale de serviciu.

MĂSURI DE PROTECȚIE A INFORMAȚIILOR NATO CLASIFICATE

Securitatea fizică reprezintă ansamblul reglementărilor, normelor și măsurilor care au drept scop prevenirea accesului ne-autorizat la informații clasificate NATO, precum și a oricăror situații, împrejurări sau fapte de natură să periclitеze ori să compromită securitatea și integritatea acestora.

Nivelurile de protecție fizică se stabilesc în funcție de următorii parametri:

a) nivelul de clasificare a informațiilor;

b) volumul și suportul fizic de prezentare a informațiilor clasificate NATO;

c) nivelul de acces conferit de certificatul de securitate, cu aplicarea principiului „nevoii de știi" („*need-to-know*");

d) situația din zona de localizare a obiectivului, delimitat de totalitatea zonelor de securitate în care sunt gestionate informații clasificate NATO.

Securitatea personalului reprezintă ansamblul procedurilor de securitate care se aplică persoanelor care urmează să aibă acces la informații clasificate NATO.

Măsurile de securitate a personalului sunt menite: să prevină accesul persoanelor ne-autorizate la informații clasificate NATO; să garanteze că informațiile clasificate NATO sunt distribuite pe baza existenței certificatului de securitate, exclusiv pe baza principiului „nevoii de a ști"; să permită identificarea persoanelor care, prin acțiunile lor, pot pune

în pericol securitatea informațiilor NATO și să interzică accesul acestor persoane la astfel de informații.

Asigurarea securității personalului se realizează prin următoarele elemente: selecționarea, verificarea, avizarea și autorizarea accesului la informațiile clasificate NATO, revalidarea, retragerea certificatului, controlul și instruirea personalului.

Persoanele care fac obiectul verificărilor de securitate sunt cele care prin natura funcției sau activității lor necesită ori urmează să aibă acces la informațiile clasificate, trebuie să participe la activitățile NATO sau să lucreze în cadrul unui contract clasificat NATO.

SECURITATEA DOCUMENTELOR

Informațiile clasificate NATO necesită o protecție specifică și sunt vehiculate în conformitate cu principiul „nevoii de a ști" fără a fi menționat deținătorul original, ci doar specificând „NATO". Informația inițială rămâne proprietatea deținătorului original, care este singura autoritate care decide asupra nivelului de clasificare și diseminării acesteia, și nu poate fi transmisă unui alt stat care nu este stat membru sau unei organizații internaționale decât cu acordul proprietarului.

Clasificarea informațiilor NATO este necesară pentru a indica gradul de sensibilitate al informațiilor și, în consecință, nivelul care trebuie atribuit pentru a determina complexitatea măsurilor și procedurilor care se impun în vederea protecției respectivelor informații împotriva dezvăluirii ne-autorizate.

Nivelurile de clasificare impun, pe de o parte, asigurarea măsurilor de securitate în conformitate cu standardele NATO pentru protejarea informațiilor, iar pe de altă parte controlul accesului la respectivele informații.

Responsabilitatea încadrării informațiilor și a materialelor într-o categorie de clasificare revine deținătorului originar al informațiilor/materialelor și se face în funcție de importanța și conținutul acestora.

Potrivit riscurilor generate de divulgarea ne-autorizată a informațiilor clasificate NATO, nivelurile de clasificare se

atribuie în mod corespunzător importanței acestora și au următoarea semnificație:

– NATO/RESTRICTED — SECRET DE SERVICIU: nivel de clasificare care se aplică acelor informații și materiale a căror divulgare ne-autorizată va fi în dezavantajul intereselor NATO și al celor naționale;

– NATO/CONFIDENTIAL — SECRET: nivel de clasificare care se aplică informațiilor și materialelor a căror divulgare ne-autorizată va provoca prejudicii intereselor NATO și celor naționale;

– NATO/SECRET — STRICT SECRET: nivel de clasificare care se aplică doar informațiilor și materialelor a căror divulgare ne-autorizată va genera prejudicii grave la adresa NATO și a intereselor naționale;

– NATO/TOP SECRET — STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ: nivel de clasificare care se aplică doar informațiilor și materialelor a căror divulgare ar putea determina prejudicii extrem de grave la adresa NATO și a intereselor naționale.

Securitatea industrială se referă la ansamblul măsurilor de protecție a informațiilor vehiculate în domeniul industrial, în legătură cu licitarea, negocierea și derularea unui contract clasificat.

Un contract clasificat este un contract încheiat în condiții legale, în cadrul căruia se cuprind și se vehiculează informații clasificate.

Securitatea industrială stabilește politica de securitate pentru negocierea, încheierea și derularea contractelor clasificate, pentru stabilirea anexelor de securitate la contractele clasificate și privitor la transmiterea informațiilor clasificate în cadrul contractelor clasificate.

Participarea la negocieri în vederea încheierii unui contract clasificat este permisă în baza unei autorizații de securitate industriale, eliberată în urma unor verificări specifice, care confirmă aplicarea măsurilor minime de securitate prevăzute în standarde. Derularea unui contract clasificat de către un obiectiv industrial se realizează în baza unui certificat de securitate industrială eliberat în urma unor verificări similare.

Verificările de securitate urmăresc ca angajaţii, managerii sau proprietarii, înainte de a lua parte la o licitaţie, negociere sau la execuţia unui contract clasificat sau care presupune acces la informaţii clasificate, să deţină certificat de securitate corespunzător nivelului de clasificare a informaţiilor la care vor avea acces. Totodată, spaţiile în care se vor gestiona informaţiile clasificate (pentru licitaţie, pentru negociere, pentru analiza documentaţiilor, etc.) să fie protejate corespunzător standardelor specifice, iar obiectivul industrial să fie stabil din punct de vedere economic, să nu fie implicat în litigii care îi pot afecta această stabilitate, să-şi plătească obligaţiile financiare către stat sau către persoane fizice/juridice şi să nu prezinte riscuri de securitate.

Pentru protecţia informaţiilor clasificate NATO în domeniul industrial, sunt desemnate în calitate de autorităţi de securitate, instituţiile care, potrivit legislaţiei, au competenţa naţională în sfera civilă, respectiv militară, a sectorului industrial. În acest sens aceste autorităţi au următoarele competenţe:

– implementarea politicii de securitate naţională în domeniul industrial, îndrumarea şi acordarea asistenţei necesare în aplicarea acestei politici;

– impunerea respectării normelor de securitate industrială la nivel naţional;

– urmărirea respectării componentelor unui contract sau sub-contract clasificat NATO potrivit standardelor Alianţei Nord-Atlantice;

– la cererea unei autorităţi naţionale de securitate dintr-un stat membru NATO, eliberează certificat de securitate unui agent economic implicat în negocierea sau executarea unui contract sau sub-contract clasificat NATO;

– la cererea unei autorităţi naţionale de securitate dintr-un stat membru NATO, eliberează certificat de securitate pentru personalul implicat în negocierea sau executarea unui contract sau sub-contract clasificat NATO;

– va fi desemnată o structură-un funcţionar de securitate în obiectivele implicate în derularea contractelor şi sub-contractelor clasificate NATO, cu atribuţii specifice tipului de contract derulat.

Protecția surselor generatoare de informații (INFOSEC) este ansamblul măsurilor și structurilor destinate protecției informațiilor clasificate prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicații și al altor sisteme electronice, împotriva oricăror acțiuni care pot aduce atingere confidențialității, integrității, disponibilității și autenticității acestora.

Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum și depistarea și prevenirea amenințărilor la care sunt expuse informațiile și sistemele.

Informațiile în forma electronică reprezintă texte, date, imagini, sunete înregistrate pe suport magnetic, optic, electric sau transmise, sub formă de curenți, tensiuni ori câmp electromangnetic, în eter sau în rețelele de comunicații.

Produsul informatic de securitate reprezintă o componentă de securitate care se încorporează într-un SPAD și/sau RTD și servește la asigurarea, menținerea și sporirea confidențialității, integrității sau disponibilității/ valabilității informațiilor.

Politica de securitate se va aplica tuturor Sistemelor de Prelucrare Automată a Datelor (SPAD) și Rețelelor de Transmisii de Date (RTD), precum și Sistemelor Informatice și de Comunicații (SIC) care stochează, procesează și/sau transmit informații clasificate NATO. Aceste sisteme necesită măsuri de securitate a informațiilor, îndeosebi de control al accesului, pe baza principiul „nevoii de a ști" și a nivelului de securitate atribuit.

Prin Sistem de Prelucrare Automată a Datelor (SPAD) se înțelege un ansamblu de elemente interdependente, în care se includ: echipamentele de calcul, produsele software de bază și aplicative, metodele, procedeele și dacă este cazul, personalul, astfel organizate încât să asigure îndeplinirea funcțiilor de stocare și prelucrarea automată a informațiilor în formă electronică. Astfel de sisteme pot fi utilizate în aplicații specifice din domeniile : industrial, economic, militar, cercetare, proiectare, administrativ-organizatoric, etc.

Facilitățile de securitate specifice unui SPAD se referă la: funcții și caracteristici hardware/software; proceduri/moduri de operare; proceduri și mijloace de evidență; controlul

accesului; definirea zonei de operare a SPAD; definirea zonei de operare a posturilor de lucru/terminalelor la distanță; restricții impuse de politica de management; mijloace și structuri fizice, personal; mijloace de control ale comunicațiilor.

Toate acestea sunt necesare asigurării unui nivel acceptabil de protecție pentru informațiile clasificate care urmează să fie stocate sau procesate într-un SPAD.

Rețele de Transmisii de Date (RTD) reprezintă un ansamblu de elemente interdependente, în care se includ: dispozitive și echipamente de comunicație; tehnica de calcul hardware și software; metode și proceduri pentru transmisie-recepție date; controlul rețelei. Dacă este cazul se include și personalul aferent. Toate acestea sunt organizate astfel încât să asigure îndeplinirea funcțiilor de teletransmisie a informațiilor în formă electronică între două sau mai multe SPAD sau să permită interconectarea cu alte RTD.

RTD poate utiliza serviciile unui singur sistem de comunicații sau ale mai multor sisteme de comunicații; mai multe RTD pot utiliza serviciile unuia și aceluiași sistem de comunicații.

Facilitățile de securitate specifice unui RTD sunt specifice și cuprind: rețeaua, împreună cu toate componentele și facilitățile auxiliare unei rețele necesare pentru a asigura un nivel acceptabil de protejare pentru informațiile clasificate.

Structural, *un Sistem Informatic și de Comunicații (SIC)* reprezintă o conexiune alcătuită din cel puțin un SPAD și/sau o RTD. Prin intermediul SIC se stochează, se procesează și/sau se transmit informații sub formă electronică.

Zona SPAD reprezintă o zonă de lucru în care se găsesc și operează unul sau mai multe calculatoare, unități periferice și de stocare, mijloace de control și echipament specifice de rețea și specific comunicațiilor. Zona SPAD nu include acea zonă separată în care sunt amplasate terminale, echipamente periferice sau stații de lucru la distanță, chiar dacă aceste echipamente sunt conectate la echipamentul central de calcul din zona SPAD.

Zona terminal/stație de lucru reprezintă o zonă, separată de zona SPAD, în care se găsesc: echipamentele periferice locale sau terminale asociate echipamentului de calcul central, stațiile de lucru la distanță, echipamente de comunicații RTD.

Securitatea SPAD și/sau *RTD (SIC)* reprezintă aplicarea măsurilor de securitate la SPAD și/sau RTD cu scopul de a preveni sau împiedica atât extragerea și/sau modificarea informațiilor clasificate NATO stocate, procesate, transmise prin intermediul SPAD și/sau RTD (SIC)- prin interceptare, alterare, distrugere, accesare ne-autorizată cu mijloace electronice — cât, și invalidarea de servicii prin mijloace specifice.

Asigurarea securității SPAD și/sau RTD (SIC) presupune aplicarea unui cumul de măsuri mixte : măsuri de securitate specifice SPAD și/sau RTD, măsuri de securitate din domeniul comunicațiilor, măsuri de ordin procedural, fizice, la nivel personal și de securitate a documentelor.

Securitatea calculatoarelor (COMPUSEC) constă în aplicarea la nivel de calculator a facilităților de securitate hardware, software și firware, pentru a preveni divulgarea, manevrarea, modificarea/ștergerea ne-autorizată a informațiilor sau invalidarea ne-autorizată a unor funcții.

Securitatea comunicațiilor (COMSEC) reprezintă aplicarea măsurilor de securitate în scopul de a proteja mesajele dintr-un sistem de telecomunicații, care pot fi interceptate, studiate, analizate și care, prin reconstruire, pot conduce la dezvăluire de informații clasificate.

COMSEC reprezintă un set complex de proceduri, incluzând: măsuri de securitate a transmisiilor; măsuri de securitate împotriva emisiilor (radiațiilor); măsuri de acoperire criptologică; măsuri de securitate fizică, procedurală, de personal și a documentelor; măsuri COMPUSEC.

TEMPEST reprezintă măsuri de testare și de realizare a securității împotriva scurgerii de informații prin intermediul emisiilor electromagnetice parazite.

CONTROLUL PRIVIND PROTECȚIA INFORMAȚIILOR CLASIFICATE NATO

Controlul reprezintă activitatea de verificare a modului în care se asigură protecția informațiilor și constă în identificarea, eliminarea și contracararea oricăror riscuri de

securitate care ar duce la compromiterea, divulgarea, distrugerea sau sustragerea informațiilor clasificate NATO.

Finalitatea acțiunilor de control se constituie într-un ansamblu de măsuri și recomandări menit să asigure operaționalizarea și perfecționarea cadrului organizatoric și funcțional la toate structurile și nivelurile de activitate, cu responsabilități în protecția informațiilor clasificate NATO.

În concluzie, prin managementul informațiilor clasificate NATO ne propunem să gândim și să aplicăm toate măsurile care asigură protecția informațiilor, apărarea acestora pentru a le împiedica să ajungă la răufăcători, la inamici.

Activitatea este de mare răspundere, aș zice chiar de răspundere națională pentru că presupune o atitudine colectivă realizată prin cultivarea educației de securitate care vizează concurarea credibilității pentru activități la nivelul Alianței. Și nu-i ușor. Ea presupune oameni valoroși, serioși, responsabili, așa cum sunt cei selecționați și avizați în acest sens.

BIBLIOGRAFIE

Legea nr.51/1991 privind siguranța națională a României;
Legea nr.82/2002 privind protecția informațiilor clasificate;
HG nr. 353/15.04.2002 pentru Aprobarea Normelor privind protecția informațiilor clasificate NATO în România;
HG nr. 354/2002 privind înființarea organizrea și funcționarea Agenției de acreditare de securitate, Agenției de Securitate pentru Informatică și Comunicații și Agenției pentru Distribuirea Materialului Criptografic;
HG nr.585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România;
HG nr.781/2002 privind Protecția informațiilor de serviciu;
OUG nr.153/2002 privind organizarea și funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat;
Revista „PROFIL" editată de SRI, anul I, nr.3, octombrie 2003;
Revista „Gândirea Militară Românească", nr.6/2003.

PROTECȚIA INFORMAȚIILOR CLASIFICATE ÎN ROMÂNIA

Adrian Constantin

În contextul eforturilor generale destinate consolidării societății democratice și optimizării condițiilor necesare funcționării economiei de piață, noul cadru legislativ și conceptual-metodologic necesar protecției valorilor informaționale ale României a fost reevaluat și redefinit în raport cu obiectivele actuale și de perspectivă ale societății românești. Legea nr. 182/2002 privind protecția informațiilor clasificate instituie, în premieră în România, sistemul național de protecție a informațiilor clasificate bazat pe rațiuni circumscrise, în egală măsură, apărării valorilor definitorii ale statului român, drepturilor, libertăților și îndatoririlor fundamentale ale cetățeanului. Noul sistem instituțional aferent domeniului și standardele elaborate în aplicarea legii asigură implementarea eficientă a măsurilor necesare realizării securității protective a informațiilor clasificate și răspunde, deopotrivă, cerințelor constituționale, exigențelor euro-atlantice, realităților și intereselor societății românești. Dintr-o astfel de perspectivă, actualele reglementări în materie instituie cerințe, obligații, răspunderi și proceduri specifice raportate la diversitatea și complexitatea aspectelor cu relevanță în domeniu, în condițiile respectării liberului acces al cetățeanului la informație publică.

Cadrul conceptual în care se înscrie protecția informațiilor clasificate este fundamentat pe răspunderea directă și explicită a conducătorilor autorităților și instituțiilor publice, a agenților economici cu capital integral sau parțial de stat, a celorlalte persoane juridice de drept public sau privat deținătoare de astfel de informații și a fiecărei persoane care emite, gestionează sau intră în posesia informațiilor ce prezintă importanță din punct de vedere al securității naționale și a apărării țării.

Noul cadru legislativ în domeniul protecției informațiilor naționale și NATO/UE clasificate

Protecția informațiilor a căror divulgare neautorizată sau compromitere ar putea aduce daune securității naționale și persoanelor juridice se fundamentează pe Legea nr. 182/2002 privind protecția informațiilor clasificate. Potrivit legii, principalele obiective ale protecției informațiilor clasificate sunt: protejarea informațiilor clasificate împotriva acțiunilor de spionaj, compromitere sau acces neautorizat, a alterării sau modificării conținutului acestora, precum și împotriva sabotajelor ori distrugerilor neautorizate; realizarea securității sistemelor informatice și de transmitere a informațiilor clasificate.

Legea instituie sistemul național destinat protecției informațiilor a căror dezvăluire sau diseminare neautorizată este de natură să aducă daune securității naționale și apărării țării, respectiv să determine prejudicii unei persoane de drept public sau privat și precizează destinația măsurilor ce decurg din aplicarea sa: prevenirea accesului neautorizat la informațiile clasificate; identificarea împrejurărilor și persoanelor care, prin acțiunile lor, pot pune în pericol securitatea informațiilor clasificate; garantarea faptului că informațiile clasificate sunt distribuite exclusiv persoanelor îndreptățite, potrivit legii, să le cunoască; asigurarea protecției fizice a informațiilor, precum și a personalului necesar protecției informațiilor clasificate.

Legiuitorul a prevăzut că pentru acordarea accesului la astfel de informații, este obligatorie verificarea prealabilă a onestității și profesionalismului persoanelor care: exercită atribuții nemijlocite în domeniul protecției informațiilor clasificate; accesează informații secrete de stat; candidează la funcții publice ce implică lucrul cu asemenea informații; gestionează informații NATO, potrivit echivalenței nivelurilor de secretizare prevăzute de lege.

În același context juridic s-a stabilit că răspunderea pentru aplicarea măsurilor de protejare a informațiilor clasificate revine persoanelor autorizate care le emit, gestionează sau intră în posesia lor. Cheia mecanismului de separare a infor-

mațiilor clasificate de cele publice, o reprezintă dispozițiile art. 22 și 32 ale Legii nr. 182/2002, potrivit cărora autoritățile publice sunt obligate să-și întocmească liste proprii cuprinzând informațiile clasificate pe care le dețin — secrete de stat, pe niveluri de secretizare și, respectiv, secrete de serviciu. Listele cu informațiile secrete de stat se aprobă și se actualizează prin hotărâre a Guvernului, după care se comunică autorităților desemnate de securitate: Serviciul Român de Informații, Serviciul de Informații Externe sau celorlalte structuri informative cărora le revin sarcini de organizare a măsurilor specializate de protecție. Listele cu informații secrete de serviciu se stabilesc de către conducătorii unităților deținătoare de astfel de informații. Enunțarea obligațiilor, răspunderilor și sancțiunilor la regimul protecției informațiilor clasificate, cuprinse în Capitolul V al legii, are rolul conștientizării, din perspectiva interesului național, a acelor delimitări ce se constituie în măsuri necesare pentru protejarea valorilor naționale.

În aplicarea legii nr. 182/2002, Serviciul Român de Informații a elaborat Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin H.G. nr. 585/13.06.2002, și proiectul hotărârii de Guvern privind protecția informațiilor secrete de serviciu, aprobat prin H.G. nr. 781/25.07.2002.

Anterior adoptării Legii nr. 182/2002 au fost adoptate alte două hotărâri de Guvern, al căror obiect îl reprezintă protecția informațiilor NATO clasificate: H.G. nr. 353/15.04.2002 pentru aprobarea Normelor privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România; H.G. nr. 354/15.04.2002 privind înființarea, organizarea și funcționarea Agenției de Acreditare de Securitate, a Agenției de Securitate pentru Informatică și Comunicații și a Agenției pentru Distribuirea Materialului Criptografic.

Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin H.G. nr.585/2002, reglementează:

• clasificarea informațiilor secrete de stat și normele privind măsurile minime de protecție în cadrul fiecărei clase;

• regulile generale privind evidența, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea și distrugerea informațiilor secrete de stat;

• obligațiile și răspunderile autorităților și instituțiilor publice și ale agenților economici, ale altor persoane juridice, pentru protecția informațiilor secrete de stat;

• normele privind accesul la informații clasificate, precum și procedura verificărilor de securitate;

• condițiile de fotografiere, filmare, cartografiere și executare a unor lucrări de arte plastice în obiective sau locuri de importanță deosebită pentru protecția informațiilor secrete de stat;

• regulile privitoare la accesul străinilor la informații secrete de stat;

• regulile de identificare și marcare, inscripționările și mențiunile obligatorii pe documentele secrete de stat, în funcție de nivelulrile de secretizare, cerințele de evidență a numerelor de exemplare și a destinatarilor, termenele și regimul de păstrare, interdicțiile de reproducere și circulație;

• normele de declasare a informațiilor clasificate;

• accesul cetățenilor străini, al cetățenilor români care au și cetățenia altui stat, precum și al persoanelor apatride la informațiile secrete de stat și în locurile unde se desfășoară activități și se expun obiecte sau se execută lucrări din această categorie;

• exercitarea controlului, constatarea contravențiilor și aplicarea sancțiunilor la regimul protecției informațiilor clasificate;

Sistemul național de protecție a informațiilor clasificate

Sistemul național de protecție a informațiilor clasificate funcționează pe baza suportului legislativ și instituțional din domeniu, care asigură implementarea măsurilor de securitate juridică, procedurală, fizică, a personalului și INFOSEC în cadrul autorităților și instituțiilor publice, agenților economici cu capital integral sau parțial de stat ori altor persoane juridice de drept public sau privat deținătoare de astfel de informații.

Pentru aplicarea prevederilor legale în domeniul protecției informațiilor clasificate următoarele autorități sunt investite cu atribuții și sarcini specifice:

• *Parlamentul, Administrația Prezidențială, Guvernul și Consiliul Suprem de Apărare a Țării* stabilesc structuri și măsuri proprii privind protecția informațiilor secrete de stat, potrivit legii. Serviciul Român de Informații asigură acestor instituții asistență de specialitate;

• *Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale* stabilesc, pentru domeniile lor de activitate măsuri pentru coordonarea și controlul activității de protecție a informațiilor secrete de stat, în conformitate cu prevederile legale;

• Coordonarea activității și controlul măsurilor privitoare la protecția informațiilor secrete de stat pentru *Oficiul Central de Stat pentru Probleme Speciale și Administrația Națională a Rezervelor de Stat* se realizează de către structura specializată a Ministerului Apărării Naționale;

• *Protecția informațiilor nedestinate publicării transmise României de alte state sau de organizații internaționale,* precum și accesul la informațiile acestora se realizează în condițiile stabilite prin tratatele internaționale sau înțelegerile la care România este parte;

• *Pentru reprezentanțele României în străinătate,* coordonarea activității și controlul măsurilor privitoare la protecția informațiilor secrete de stat se realizează de către Serviciul de Informații Externe;

• Coordonarea și controlul măsurilor referitoare la protecția informațiilor secrete de stat *privind activitatea specifică a ataşaților militari din cadrul misiunilor diplomatice ale României și a reprezentanților militari pe lângă organismele internaționale,* se realizează de către Ministerul Apărării Naționale;

Oficiul Registrului Național al Informațiilor Secrete de Stat, înființat prin O.U.G. nr. 153/2002, asigură implemen-

tarea unitară, la nivel național (pe zonele de competență militară și civilă) a măsurilor de securitate a informațiilor clasificate naționale, precum și a celor care fac obiectul tratatelor, înțelegerilor și acordurilor bilaterale sau multilaterale la care România este parte.

Consiliul Suprem de Apărare a Țării asigură coordonarea, la nivel național, a programelor de protecție a informațiilor clasificate.

Serviciul Român de Informații are competență generală privind coordonarea activității și exercitarea controlului asupra măsurilor privitoare la informațiile clasificate.

SECURITATEA INDUSTRIALĂ
Experienţa nord-americană în domeniul managementului protecţiei informaţiilor clasificate transmise către industrie în cadrul contractelor clasificate

Ion Traian Mihai

Securitatea industrială reprezintă ansamblul măsurilor și procedurilor care au drept scop prevenirea pierderii sau compromiterii informațiilor clasificate gestionate în cadrul activităților contractuale și identificarea și recuperarea celor pierdute sau compromise.

Informațiile clasificate reprezintă acele informații (comunicate sub orice formă) sau materiale care necesită a fi protejate împotriva accesului neautorizat și care au fost astfel identificate de clasificările de securitate. Termenul *material* se definește astfel: documente, precum și echipamente/componente, armamente fabricate sau în curs de fabricare. Termenul *document* se definește astfel: orice informație înregistrată referitoare la formele sau caracteristicile fizice, inclusiv, fără a se limita, la materialele scrise sau tipărite, cartele și casete de procesare a datelor, hărți, diagrame, fotografii, picturi, desene, gravuri, schițe, hârtii și notițe de lucru, copii de carbon sau riboane sau reproduceri prin orice mijloace sau procese, sunet, voce, magnetic sau electronic sau înregistrare optică și video în orice formă;

Sistemul de protecție a informațiilor clasificate reprezintă totalitatea structurilor de securitate, procedurilor, dotărilor specifice, resurselor umane și materiale destinate protecției informațiilor clasificate într-o manieră unitară și eficientă.

Guvernul SUA certifică obiectivele industriale din punct de vedere al securității industriale astfel încât acestea să dețină programe bine puse la punct de protecție a informațiilor clasificate. Un certificat de securitate industrială este o decizie a Guvernului SUA că un obiectiv industrial poate

avea acces la informații clasificate și reprezintă în fapt un parteneriat între Guvern și contractant.

Serviciul de securitate al apărării (DSS) din cadrul Departamentului Apărării al SUA stabilește strategia de implementare unitară la nivel național a măsurilor de protecție a informațiilor clasificate gestionate în cadrul contractelor clasificate.

Documentul care stă la baza verificărilor de securitate și eliberării certificatului de securitate pentru personal și a certificatelor de securitate industrială este Manualul de Operare al Programului Național de Securitate Industrială (NISPOM).

Programul Național de Securitate Industrială (NISP) a fost realizat pentru a garanta că sectorul industrial privat, colegiile/universitățile, laboratoarele de cercetare, în timp ce derulează contracte guvernamentale sau realizează activități de cercetare și dezvoltare, protejează în mod corespunzător informațiile/materialele clasificate pe care le gestionează.

Până în prezent, având la bază procedurile din NISPOM, DSS a certificat aproximativ 800000 de persoane din sectorul industrial. De asemenea, DSS supraveghează și consiliază, în domeniul securității industriale, mai mult de 11000 de obiective industriale care au obținut certificatul de securitate industrială. Se estimează că mai mult de 11 milioane de documente clasificate se află în posesia sectorului industrial din SUA implicat în contracte clasificate guvernamentale.

Directorul DSS este responsabil cu administrarea Programului Național de Securitate Industrială în numele Departamentului Apărării și a altor 21 de departamente și agenții guvernamentale ce nu fac parte din Departamentul Apărării, dar care au semnat un acord cu acest Departament.

Prin politicile și procedurile pe care le implementează, DSS trebuie să garanteze că: un obiectiv industrial poate primi informații clasificate; contractantul are sisteme de securitate capabile să protejeze informațiile clasificate ce i-au fost încredințate.

PROCEDURA DE ELIBERARE A CERTIFICATELOR DE SECURITATE INDUSTRIAL

Termenul de obiectiv industrial este folosit, în cadrul NISPOM, ca o denumire a unei entități ce este reprezentată de o fabrică, laborator, birou, colegiu, universitate sau structură comercială cu depozit aferent, locații de depozitare, utilități și componente care sunt legate prin funcție sau locație și nu se referă la facilități aparținând Guvernului SUA.

Un certificat de securitate industrială (CSI) este un document administrativ care, din punct de vedere al securității naționale, atestă că un obiectiv industrial poate avea acces la informații clasificate de nivel egal sau mai mic decât nivelul de clasificare pentru care a fost autorizat. CSI poate fi acordat pentru nivelul CONFIDENTIAL, SECRET sau TOP SECRET.

Eliberarea CSI presupune respectarea unui Acord de Securitate încheiat de contractanți cu Departamentul Apărării al SUA. Conform acordului, Guvernul SUA este de acord să elibereze CSI și să informeze contractantul asupra clasificării de securitate a informațiilor la care va avea acces. În schimb, contractantul este de acord să respecte cerințele de securitate stabilite de NISPOM.

Un contractant sau posibil contractant nu poate solicita în nume propriu un certificat de securitate industrială. Un departament sau o agenție a Guvernului SUA sau un contractant care a fost autorizat anterior, în cazul sub-contractării, poate solicita un certificat de securitate industrială pentru un alt obiectiv industrial atunci când s-a stabilit că acest lucru este necesar.

La fel ca în cazul unei activități neclasificate, obiectivul industrial trebuie să devină licitator la o activitate a Guvernului SUA sau a unui contractor sau sub-contractor care desfășoară un contract clasificat. În cazul în care o licitație sau un posibil sub-contract presupune acces la informații clasificate, contractorul ce deține CSI solicită autorizarea posibilului participant la licitație. Personal din cadrul Biroului de Certificare de Securitate Industrială (DISCO) evaluează

cererea și se asigură că aceasta este validă. O parte a acestei validări include confirmarea faptului că obiectivul industrial are o reputație a integrității și a bunei desfășurări a activităților de afaceri în care este implicat. Mai mult, contractantul și persoanele din top-managementul acestuia nu trebuie să fi fost excluși anterior de la participarea în alte contracte guvernamentale.

După stabilirea validității cererii, procesarea informațiilor se va face de către un birou de securitate industrială a DSS. Ulterior, obiectivul industrial este atribuit unui reprezentant de securitate industrială a DSS. Acesta obține informații despre obiectivul industrial și pune la dispoziția acestuia instrucțiuni de completare a formelor necesare oferind informațiile principale despre NISP. De asemenea, asigură consultanță obiectivului industrial în vederea stabilirii unui program de securitate industrială.

Eliberarea certificatului de securitate industrială nu implică costuri directe pentru contractant. Contractantul este responsabil pentru costurile de securitate implicate de implementarea NISPOM. Prin urmare, contractanții trebuie să-și determine cerințele de securitate proprii și costurile aferente și să ia în considerare aceste costuri atunci când participă la o licitație. Reprezentantul DSS poate consilia obiectivul industrial în vederea determinării cerințelor de securitate necesare.

NISPON stabilește cerințele de securitate minime care trebuie îndeplinite de contractanții certificați. Implementarea acestor cerințe va asigura protejarea adecvată a informațiilor clasificate implicate. În unele cazuri, agențiile sau departamentele guvernamentale (beneficiarele contractului clasificat) pot solicita cerințe de securitate suplimentare.

Certificatul de securitate industrială este valid atâta timp cât Acordul de Securitate încheiat între contractant și DSS este valid. Acest acord poate fi denunțat de orice parte cu o notificare prealabilă de 30 de zile. În general, marea majoritate a certificatelor de securitate industrială sunt valide atâta timp cât contractantul are nevoie de acces la informații clasificate.

Periodic se vor desfășura inspecții de securitate conduse de reprezentantul de securitate industrială al DSS la toți contractanții certificați. Acesta va stabili frecvența desfășurării unor astfel de inspecții care, în mod normal, sunt anuale.

Sarcinile reprezentantului de securitate industrială a DSS pot fi sistematizate astfel: instruiește angajații contractantului, care vor proteja informații clasificate; aprobă containerele/încăperile de securitate pentru depozitarea informațiilor clasificate; sprijină contractantul în procesul acreditării sistemelor informatice care procesează informații clasificate; acordă, la cerere, consiliere și asistență funcționarului de securitate și angajaților contractantului; asistă contractantul în investigarea cazurilor de încălcare a procedurilor de securitate, constatarea cazurilor de compromitere a informațiilor și inițierea de proceduri pentru atenuarea consecințelor; asigură transferul informațiilor clasificate între guverne diferite pe baza acordurilor bilaterale; analizează anual programul contractantului de protecție a informațiilor clasificate.

COMPONENTELE SISTEMULUI DE PROTECȚIE A INFORMAȚIILOR CLASIFICATE

Componentele care concură la certificarea din punct de vedere al securității industriale a companiilor implicate în derularea unor contracte clasificate sunt următoarele: securitatea personalului; securitatea fizică și a documentelor; protecția informațiilor clasificate procesate, stocate sau transmise prin intermediul mediilor electronice și de comunicație — INFOSEC.

Securitatea personalului. Un certificat de securitate pentru personal este un document administrativ care confirmă că un angajat al unui obiectiv industrial este eligibil pentru accesul la informații clasificate.

Acest document are la bază o investigație și o analiză a datelor personale ale celui verificat și confirmă că accesul la informații clasificate este în conformitate cu interesele naționale ale SUA.

Departamentul Apărării eliberează certificate de securitate pentru personal pentru cetățenii SUA angajați ai unui contractant care necesită acces la informații clasificate. Certificatele se eliberează pe trei niveluri: TOP SECRET, SECRET și CONFIDENTIAL. Cererile de eliberare a certificatelor de securitate pentru personal sunt trimise către Biroul de Certificare de Securitate Industrială (DISCO) din cadrul Departamentului Apărării, care eliberează aceste certificate.

Persoanele care nu sunt cetățeni ai SUA nu pot primi certificate de securitate pentru acces la informații clasificate ale SUA. În situații foarte rare, ca o excepție de la această regulă, persoane care nu au cetățenie SUA dar care posedă calități și cunoștințe vitale pentru derularea unui contract clasificat pot primi o Autorizație de Acces Limitat pentru accesul la informații clasificate.

Contractantul nu poate acorda, retrage sau revoca certificatul de securitate al unui angajat, acest lucru fiind rezervat numai Guvernului SUA.

Securitatea fizică și a documentelor. În opinia experților SUA, protecția obiectivelor industriale (securitatea fizică) este unul din sub-sistemele principale pentru implementarea unui program de securitate eficient.

Sistemul securității fizice trebuie să protejeze împotriva accesului neautorizat, să detecteze orice încercare neautorizată de acces și să poată răspunde în consecință. Protecția implică bariere de ordin fizic, procedural și psihologic pentru întârziere sau distrugere.

Detectarea se referă la dispozitive și metode ce au rolul de a arăta și, dacă este posibil, de a verifica orice acces neautorizat prezent sau suspectat. Răspunsul se referă la reacții cum ar fi implicarea forțelor de pază sau poliție, evaluarea pagubelor și luarea măsurilor de prevenire a deteriorării altor elemente ale sistemului.

Aproape orice măsură de securitate fizică poate fi compromisă, dacă este timp suficient. De aceea este important ca măsurile de siguranță să fie create în așa fel încât ele să nu poată fi compromise până în momentul în care o persoană

sau unitate ajunge la fața locului. Reprezentantul de securitate industrială din cadrul DSS asigură asistență și consiliere pentru dezvoltarea unui plan de protecție al obiectivului industrial.

Protecția informațiilor clasificate procesate, stocate sau transmise prin intermediul mediilor electronice și de comunicație — INFOSEC. Sistemele Informatice (SI) folosite pentru crearea, procesarea sau distribuirea documentelor clasificate trebuie protejate împotriva diseminării neautorizate de informații clasificate, pierderea integrității datelor și pentru asigurarea valabilității datelor și sistemului.

Autoritatea Desemnată de Acreditare (ACS) este responsabilă pentru acreditarea sistemelor informatice folosite la procesarea informațiilor clasificate în industrie.

Procesul de certificare și acreditare este o parte integrantă a ciclului de viață a unui SI. Certificarea validează că măsurile de protecție au fost implementate în sistem și funcționează corect. Acreditarea reprezintă aprobarea ACS pentru ca sistemul să poată procesa informații clasificate.

Personalul cu acces la sistemul informatic joacă un rol esențial în protejarea informațiilor; definind sistemul lor de politici de securitate și menținând și monitorizând confidențialitatea, integritatea și valabilitatea atributelor stocate în SI. Îndatoririle, responsabilitățile, privilegiile și limitările specifice ale utilizatorilor SI, utilizatori ordinari sau privilegiați, vor fi specificate în scris. Atâta timp cât este posibil, datoriile de securitate vor fi distribuite pentru a preveni orice individ să afecteze diferite operațiuni sau integritatea sistemului. Nivelurile de protecție pentru diferitele SI vor fi determinate de nivelurile de clasificare, aprobările oficiale de acces și necesitatea de a cunoaște a utilizatorilor SI și nivelul de clasificare al datelor procesate sau stocate.

Deținerea, controlul sau influențarea unui obiectiv industrial de către interese străine (FOCI) — particularitate a sistemului nord-american de protecție a informațiilor clasificate transmise către industrie

Termenul FOCI este utilizat atunci când un acționar din afara SUA are puterea, directă sau indirectă, chiar dacă nu

şi-o exercită, de a decide în problemele ce afectează managementul sau operaţiunile companiei într-un mod care ar conduce la accesul neautorizat la informaţii clasificate sau care poate afecta în mod negativ derularea unor contracte clasificate.

În cadrul procesului de verificare pentru eliberarea certificatului de securitate industrială, managementul companiei trebuie să completeze un formular cu 10 întrebări care clarifică existenţa unui asemenea acţionar în cadrul companiei. Mai mult, pe timpul valabilităţii certificatului de securitate industrială managementul companiei trebuie să informeze cu privire la orice schimbare care apare în ceea ce priveşte acest aspect.

Atunci când se constată că o companie este sub influenţă străină nu i se acordă certificatul de securitate industrială până când nu se implementează măsuri speciale de securitate stabilite de DSS care să înlăture posibilitatea accesului neautorizat la informaţii clasificate sau afectarea contractelor clasificate.

CONCLUZII

Cele mai importante concluzii desprinse din studiul legislaţiei nord-americane în domeniul securităţii industriale pot fi redate sub forma unor principii, după cum urmează:

- Informaţiile clasificate sunt emise şi deţinute de Guvernul SUA fiind puse la dispoziţia companiilor exclusiv pentru realizarea unor nevoi guvernamentale;
- Derularea de contracte clasificate ale SUA este permisă numai contractanţilor, persoane juridice, care îşi desfăşoară activitatea sub legile SUA, sunt localizaţi în SUA sau în posesiunile teritoriale ale acestora;
- Accesul la informaţiile clasificate este permis numai cetăţenilor SUA şi numai în cazuri excepţionale cetăţenilor de altă naţionalitate;

• Analiza amănunțită a acelor situații în care există acționari străini în companii care derulează contracte clasificate, pentru limitarea accesului la informații clasificate;

• Certificarea încă din faza inițială a tuturor persoanelor din conducerea unei companii ce urmează a fi implicată în derularea unor contracte clasificate.

BIBLIOGRAFIE

1. *Manualul de Operare al Programului Național de Securitate Industrială*, Departamentul Apărării al SUA, 1995.
2. *Anexa COMSEC la Manualul de Operare al Programului Național de Securitate Industrială*, Departamentul Apărării al SUA, 1995.
3. *Manualul COMSEC de securitate industrială*, Agenția Națională de Securitate a SUA, 2001.
4. *Directivele DSS privind securitatea industrială*, Departamentul Apărării al SUA.
5. Legea nr. 182/2002 privind protecția informațiilor clasificate.
6. Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord aprobate prin Hotărârea Guvernului nr. 353/2002.

V. ALTE PROBLEME DE SECURITATE ȘI SIGURANȚĂ NAȚIONALĂ

RĂZBOIUL INFORMAȚIONAL ȘI SECURITATEA NAȚIONALĂ

Ionel Lanciu

- Informația pe care o ai nu este cea pe care o vrei;
- Informația pe care o vrei nu este cea de care ai nevoie;
- Informația de care ai nevoie nu este cea pe care o poți obține;
- Informația pe care o poți obține costă mai mult decât poți să plătești.

Murphy (Legile informației)

Una dintre consecințele dispariției sistemului bipolar (a ordinii internaționale bazate pe logica echilibrului de puteri) și exploziei tehnologice actuale o reprezintă preocuparea tot mai mare pe care statele o acordă *războiului informațional* (*R.I.*)[119], ca „război politic", ca parte componentă a politicii statului, atât pentru promovarea cât și pentru protejarea intereselor naționale.

Teoria și practica *războiului informațional și operațiilor informaționale* se bucură, în ultimul timp, de o atenție crescândă din partea politicienilor, strategilor, oamenilor de știință și mijloacelor de informare în masă din diverse țări, îndeosebi din spațiul nord-atlantic și european, fenomen ușor

[119] Oficial, conceptul de R.I. a fost lansat în Statele Unite, în decembrie 1992 (la aproape doi ani de la războiul din Golf, considerat a fi „războiul pilot" în care s-au folosit mijloace specifice R.I.). În septembrie 1995, Departamentul Apărării a publicat prima definiție oficială a R.I.: *„acțiunile întreprinse pentru a obține superioritatea informațională, prin afectarea informațiilor adversarului, a proceselor și sistemelor informaționale în paralel cu acțiunile întreprinse pentru a apăra propriile informații, procese și sisteme informaționale"*.

de constatat urmărind frecvența discursurilor publice, conferințelor, simpozioanelor, cărților, studiilor și articolelor care abordează această problemă.

Importanța actuală a acestui domeniu în politica, strategia și tactica militară este similară cu importanța logisticii în cel de al doilea război mondial. Mediile politico-militare și civile occidentale parafrazează deja două maxime celebre: *„Nu știu ce este R.I., dar îl vreau!"*; *„Un general se ocupă de strategie, un general bun de R.I."*

Caracteristica de subiect „fierbinte" și important este, de asemenea, relevată de diversitatea și exotismul unor *concepte* (infrastructură informațională critică, operații informaționale), *specializări universitare* (strategie cibernetică), *instituții* (Colegiul de Management al Resurselor Informaționale), *preocupări* („hacker", „cracker"), toate asociate domeniului R.I.

RĂZBOIUL INFORMAȚIONAL. REPERE CONCEPTUALE

Conceptul de război a evoluat odată cu progresul culturii societăților, nivelului lor tehnologic, valorilor și infrastructurii lor. Societatea începutului de secol XXI — societate globală, hipermediatizată, computerizată — se îndreaptă spre un *război al informației.*

Una dintre consecințele exploziei tehnologiei de vârf este atenția din ce în ce mai mare pe care statele o acordă R.I., atât ca mijloc de protejare a intereselor naționale, cât și ca instrument de atac (formal, R.I. a fost lansat în Statele Unite, în decembrie 1992 în momentul apariției directivei 3600.1. a Ministerului american al Apărării).

R.I. este un concept care, deși nu posedă o definiție universal acceptată, încearcă să ofere o anumită coerență unor activități care n-o posedă. Putem vorbi de R.I. ca fiind o manieră nouă de a purta un război, dacă ne referim la mijloacele sale (ce utilizează tehnologii sofisticate) și în același timp veche, dacă avem în vedere conceptele pe care se sprijină (a înșela, a amăgi, a dezinforma, a manipula, a controla, a modifica percepția adversarului, prin orice mijloace, asupra situa-

ției date pentru a-i influența comportamentul, reacțiile și deciziile, în cele din urmă).

Practic R.I. a evoluat în ultimii ani și a dezvoltat un concept „atotcuprinzător", care pe lângă activitățile practicate din totdeauna (înșelătorie, propagandă, operații psihologice, atacuri fizice), include noi forme de război, ca războiul electronic sau războiul hackerilor, determinate de progresele tehnologice.

Unele aspecte, caracteristice conceptului de R.I., sunt la fel de vechi ca și societatea umană. Oamenii au avut nevoie din totdeauna de informații, pe care au încercat să le culeagă, să le coreleze, să le stocheze și să le utilizeze prin metode și mijloace specifice timpului respectiv.

În toate epocile au existat acțiuni de manipulare, de inducere în eroare. În totdeauna s-a simțit nevoia cunoașterii adversarului (sau a aliatului) și luării unor decizii, în funcție de informațiile avute la dispoziție.

Totuși nu se poate vorbi de R.I. pentru a caracteriza acțiunile întreprinse în trecut, deoarece: informația, în general, nu era considerată o armă, un mijloc de acțiune; manipularea, inducerea în eroare, distrugerea fizică etc., nu erau corelate, iar finalitatea lor era una practică, nu viza în mod sistematic atacul informațiilor adversarului, protejarea propriilor informații, respectiv influențarea voinței și a modului de gândire al adversarului.

Ceea ce este nou și caracteristic R.I., este posibilitatea de a manipula informația vehiculată în sistemele informaționale și uneltele necesare pentru a forma și orienta această informație.

Informația a devenit o adevărată *materie primă strategică,* indispensabilă formulării deciziei și succesului oricărei politici.

În mediile științifice și universitare și în literatura preponderent militară, există numeroase definiții, mai mult sau mai puțin cuprinzătoare, ale R.I.

Încercând să circumscrie conținutul și caracteristicile acestui concept, definițiile pun accentul pe faptul că acest tip de război se bazează pe *acțiuni defensive și ofensive, integrate într-o strategie globală* (care presupune nu doar o serie de mijloace tehnice, ci și un ansamblu de *operații informaționale*, care

să îmbine tehnicile și informațiile deținute în funcție de un anumit scop).

Înțelegerea corectă a ceea ce înseamnă R.I., în accepțiunea actuală a termenului, necesită unele clarificări.

R.I. nu este o formă exclusiv militară de conflict, acesta vizând scopuri și angajând resurse și activități care, în funcție de context, pot depăși cu mult sfera strictă a domeniului militar.

În general, R.I. cuprinde acțiuni care se pot desfășura atât pe timp de pace sau de război — în perioade calificate ca atare din punct de vedere juridic — cât și în perioade de criză. Există o recunoaștere tacită privind desfășurarea operațiilor informaționale, îndeosebi pe timp de pace.

De asemenea, R.I. poate constitui o strategie integratoare, care să subordoneze toate celelalte strategii operaționale indiferent de domeniul lor de aplicabilitate, dar poate fi și subordonat scopurilor unei anumite strategii.

Există multe încercări de definire a R.I. În esență, toate aceste definiții surprind faptul că:

R.I. reprezintă totalitatea acțiunilor desfășurate pentru afectarea informațiilor unui adversar sau aliat, a proceselor și sistemelor sale informaționale, concomitent cu protejarea propriilor informații și a propriilor procese și sisteme informaționale.

Scopul general al R.I. îl reprezintă cucerirea și menținerea superiorității informaționale.

Pentru satisfacerea intereselor de securitate națională, dominarea spectrului de informații este la fel de critică, precum era și este încă ocuparea terenului sau dominarea spațiului aerian, în strategia militară.

La nivel de stat, R.I. îmbracă șapte forme: războiul de comandă-control (forma exclusiv militară a R.I.); războiul electronic; războiul sistemelor informative (*intelligence*); războiul psihologic; războiul informațiilor economice; războiul hacker-ilor; războiul în spațiul realității virtuale. Cea din urmă constituie în prezent un „punct de acumulare" pentru cercetarea tehnologică și fundamentală și pentru unele scenarii futuriste. Indiferent de forma pe care o îmbracă la

un moment dat, R.I. se sprijină pe rezultatele activității comunității informative a statului.

Atingerea obiectivelor specifice R.I. se realizează prin desfășurarea operațiilor informaționale, pe timp de pace, criză sau conflict, care pot fi ofensive și defensive. Atât operațiile informaționale ofensive, cât și cele defensive cuprind elemente cum sunt: operații psihologice; acțiuni de război electronic; acțiuni de inducere în eroare; securitatea operațiilor, siguranța informațională; acțiuni de atac și/sau distrugere fizică; acțiuni din sfera relațiilor publice și relațiilor militari-civili.

În acest punct, sunt necesare câteva precizări importante. În sens larg, *R.I. este purtat la nivelul întregii societăți, între organizații și chiar între indivizi, care urmăresc permanent obținerea unei superiorități informaționale față de adversari și chiar față de parteneri.* În sens restrâns, *R.I. reprezintă ansamblul acțiunilor care vizează obținerea superiorității informaționale în perioada de război, recunoscută juridic ca atare.*

R.I. este însoțit de noi mijloace de acțiune/influențare care eludează puterea convențională și granițele statelor. Multe dintre aceste mijloace acționează direct la nivelul comenzii și al controlului, al voinței, al informației, precum și asupra elementelor esențiale ale infrastructurii statale.

De asemenea, R.I. urmărește evitarea conflictelor convenționale, a producerii de victime și pagube, prin utilizarea acestor noi mijloace aflate la granița dintre starea convențională de război și starea convențională de pace.

R.I. vizează structuri ale domeniului politic, economic, social sau militar, nu doar pentru a le distruge sau paraliza ci mai ales, pentru a le influența procesele decizionale. Astfel, se face trecerea de la stadiul de violență organizată la stadiul de influențare ostilă.

R.I. redimensionează noțiunea de conflict-competiție adăugându-i noi atribute: *permanență, transversalitate și dualitate.*

Permanența presupune că aplicarea unei strategii globale care integrează colectarea, protecția, transportul și managementul accesului la informație nu se limitează numai la perioadele de criză sau conflict.

Transversalitatea semnifică influențarea societății în ansamblul ei, având la bază conceptele de „sistem de sisteme" și de multidisciplinaritate.

Dualitatea se referă la dispariția deosebirilor dintre sfera militară și cea civilă. Statele și forțele armate nu vor mai avea monopolul absolut asupra mijloacelor violente și îndeosebi asupra „violenței informaționale". Centrul de greutate strategic (național) se va muta treptat în domeniul bancar, financiar, energetic și al sistemelor de distribuție.

Multe lucrări tratează războiul informațional și războiul erei informaționale în același mod. *Războiul erei informaționale utilizează tehnologia informațională ca mijloc de realizare a unei economii de timp și forțe și ca mijloc de eficientizare a acțiunilor. Războiul informațional utilizează informația ca armă și/sau obiectiv.* Legătura dintre cele două sintagme constă în faptul că tehnologia erei informaționale permite manipularea directă a informațiilor de care dispune adversarul.

Dezvoltarea tehnologiilor informaționale schimbă, azi, nu numai noțiunea de „război" dar și modul de „a face război". Dacă înainte se punea accent mai ales pe distrugerea fizică a adversarului, acum se dorește controlul, anihilarea, neutralizarea lui, tocmai printr-o *superioritate informațională*, evitându-se din ce în ce mai des recurgerea la o confruntare armată directă.

Percepția asupra ideii de „război" începe să se modifice odată cu explozia tehnologiilor sofisticate, noțiunea de „război" nemaifiind neapărat sinonimă cu cea de „conflict", adică cu cea de „acțiuni armate".

Războiul, în zilele noastre, și-a deplasat sfera de interes către noile domenii, în care se joacă supremația planetară: economic, informațional, rețele de infrastructură etc.

După cum am mai spus, R.I. nu constituie o practică nouă. A fost utilizat și în timpul celui de-al doilea Război mondial. Noutatea pe care o aduce azi constă în includerea mijloacelor tehnice sofisticate într-o *strategie globală*, în funcție de scopul urmărit.

R.I. nu are nevoie doar de o strategie care să îmbine mijloacele (resursele: bani, materiale, logistică, armate etc.)

necesare pentru a fi sprijinit, ci și de o definire a scopurilor sale (influențarea factorilor de decizie, informația, procesele informaționale sau sistemele de informare și comunicare), scopuri ce derivă din interesele naționale și/sau particulare. Trebuie remarcat că în momentul de față, în afară de protejarea infrastructurii naționale de informații (sistemele radar, sistemele de poștă și telecomunicații, comunicațiile aviației civile, militare, sistemele de distribuire a energiei electrice, a apei, a gazului etc.) alte obiective naționale nu sunt ușor de definit, referindu-ne strict la R.I. Protejarea acestei infrastructuri critice e greu de realizat.

Trebuie înțeles faptul că, *fenomenul R.I. și securitatea informațională nu constituie doar o problemă a altor state, a celor avansate tehnologic, și prin urmare, trebuie să devină o preocupare națională, permanentă.* Pe de altă parte, *nu este o problemă ce afectează doar un anumit domeniu, ci întreaga societate, de la instituții la indivizi.*

Modificările importante în privința naturii și diversității amenințărilor, corelate cu dezvoltarea în România (într-un stadiu embrionar) a caracteristicilor specifice societății informaționale (interconectarea, impactul tehnologiei informației — creșterea capacității de procesare, stocare și transmitere a informațiilor, ceea ce conduce la performanță, reacții rapide etc. — creșterea numărului și a diversității surselor de informare, precum și a volumului și valorii informațiilor puse la dispoziție, apariția unor factori de risc specifici societății informaționale) fac necesară stimularea procesul de luare a unor măsuri în domeniul politic, economic, militar, juridic.

CATEGORII DE ȚINTE ALE RĂZBOIULUI INFORMAȚIONAL

În sfera militară, sistemele informaționale cuprind sistemele de comandă și control, sistemele informatice, sistemele platformelor de cercetare-lovire și rețelele de comunicații, toate acestea constituind infrastructura informațională militară critică.

Sfera civilă posedă și ea echivalentul acestor sisteme critice pentru securitatea națională (centrele de decizie de la nivel politic, economic, religios, social, de exemplu; infrastructura națională: sistemele de alimentare cu apă potabilă, cu energie, cu gaz; sistemele bancare, sistemele de telecomunicație etc.). Practic aceste sisteme informaționale (militare și civile) se sprijină reciproc și, frecvent, utilizează aceeași infrastructură informațională.

Importanța acestor infrastructuri informaționale este evidentă în cazul RI. Așa cum se remarcă în studiile de specialitate se pot distinge trei niveluri de ținte ale unui atac informațional:

• *Nivelul sistemelor informaționale.* Neglijând obiectivul principal, atacurile R.I. se îndreaptă, deseori, asupra sistemului informațional care nu întotdeauna reprezintă un sistem electronic. În multe cazuri, acest sistem este ținta inițială a atacului, efectele fiind de natură tehnică (supraâncărcarea sursei de recepție, coruperea datelor, stricarea computerelor, distrugeri fizice etc.). Acest punct este des întâlnit în literatura de specialitate, discuțiile despre R.I. concentrându-se asupra țintelor și metodelor de atac tehnic. Ceea ce nu se are în vedere este obținerea efectelor operaționale.

• *Nivelul gestionării informației.* Gestionarea informației se referă la transferul informației, răspândirea, stocarea ei. Efectele sunt funcționale: o întârziere a informației sau o schimbare la nivelul capacităților de transfer al informației.

• *Nivelul procesului de decizie.* Efectele operaționale ale atacului R.I. de la acest nivel pot fi indirecte: nu se dorește doar producerea confuziei ci și formarea, influențarea deciziilor, opiniilor adversarului.

Efectele la un anumit nivel generează efecte la nivelul superior, dar pot și produce direct un efect operațional. Scopul final al unei campanii de R.I. îl reprezintă nivelul procesului decizional. Așa cum este sugerat și în figura 1, există multiple căi de a ataca procesul de decizie.

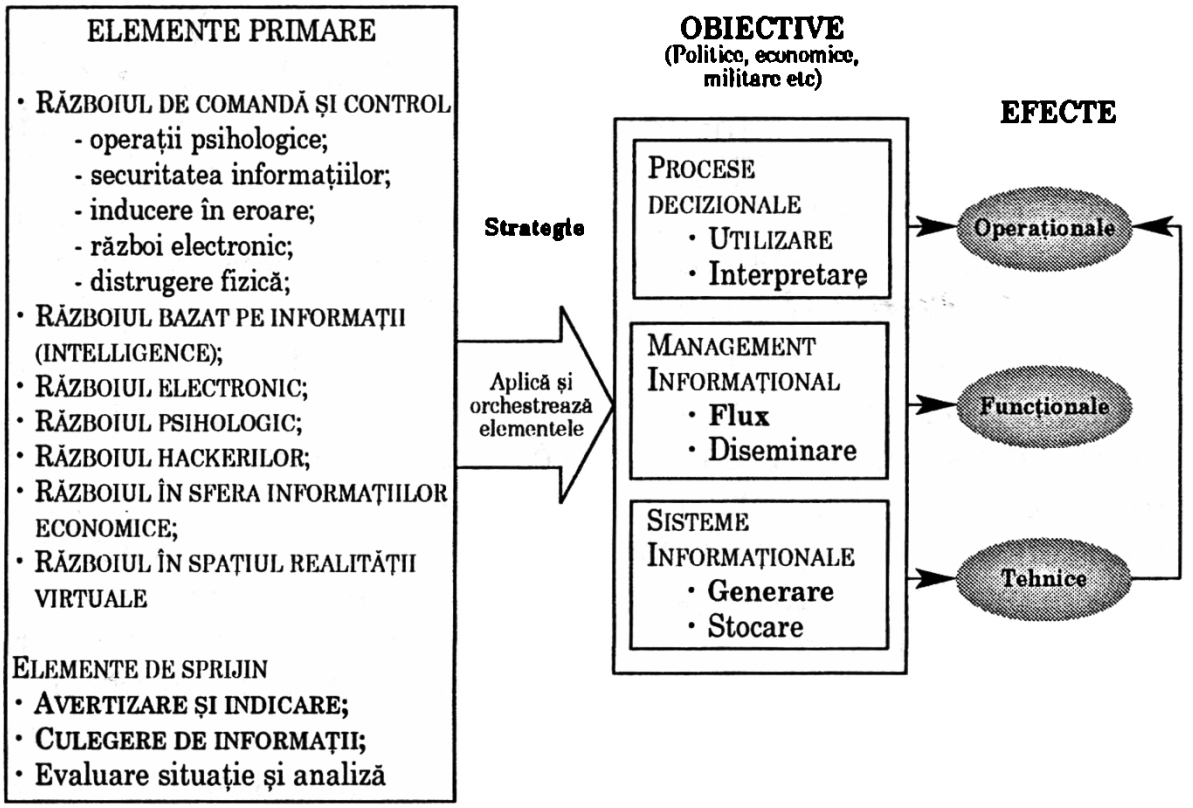


Figura 1 **Model generic al RI**

INFRASTRUCTURILE CRITICE ÎN RĂZBOIUL INFORMAŢIONAL

Când se vorbeşte de orientarea spre ţintă în contextul R.I., se fac, de obicei, analogii directe cu războiul cinetic, specific erei industriale: atacuri asupra infrastructurii critice, atacuri asupra sistemelor de comandă şi control etc. Acum sunt avute în vedere şi atacurile asupra computerelor şi sistemelor informaţionale.

La nivelul strategic al analizei, sectoarele infrastructurii critice reprezintă „organele vitale" ale societăţii. În era informaţională, problema care se pune este aceea dacă aceste aspecte ar trebui sau nu să intre în responsabilitatea armatei.

Acestea nu numai că sunt esenţiale bunăstării economice ale oricărei societăţi evoluate, dar ele sunt din ce în ce mai importante pentru viabilitatea forţelor armate ale ţării respective. Sectoarele civil şi militar se suprapun din ce în ce mai mult. Sectoarele infrastructurii critice includ: siste-

mele și rețelele de comunicații terestre și spațiale; sistemele și rețelele de transport; sistemele și rețelele de distribuție a energiei; sistemele bancar și financiar; sistemele de distribuție, rafinare și purificare a apei; serviciile guvernamentale esențiale; serviciile de urgență (poliție, pompieri, salvare).

În societățile cele mai evoluate, aceste servicii sunt o responsabilitate împărțită de către sectoarele public și privat. Dar indiferent de cine le posedă, aceste sectoare ale infrastructurii au în comun un element esențial: faptul că sunt informatizate într-o măsură din ce în ce mai mare. Progresele în materie de informatică au fost folosite pentru îmbunătățirea și eficientizarea serviciilor infrastructurii și reducerea costurilor operaționale. Însă, pe măsură ce se favorizează eficiența infrastructurilor critice, se mărește și vulnerabilitatea lor.

Referitor la protecția infrastructurii critice, trebuie luate în considerare patru aspecte ale amenințării: riscul sinergic; amenințarea asimetrică; amenințarea asincronă; criza de încredere.

Statele-națiune sunt, în principiu, „sisteme de sisteme" elaborate și complexe. Cu cât națiunea este mai avansată din punct de vedere economic, cu atât relațiile infrastructurii sunt mai complexe. Distrugerea sau afectarea gravă a sectorului infrastructurii critice are imediat efecte adverse asupra celorlalte sectoare, și nu doar la nivel național. Întrucât sistemele și sub-sistemele infrastructurii sunt interdependente într-o măsură din ce în ce mai mare, ele nu pot fi segregate sau izolate într-un efort de limitare a pagubelor.

Preocuparea pentru *amenințările asimetrice* la nivel strategic și tactic este deosebit de relevantă pentru aspectul protecției infrastructurii. O putere mai mică (statală sau non-statală) poate produce mari pagube unei națiuni mai robuste, dată fiind dependența sporită a acesteia din urmă de infrastructurile critice. Altfel spus, o societate mai puțin dezvoltată este mai puțin dependentă de aceste sisteme atât fizic, cât și psihologic.

O *amenințare asincronă* poate fi și ea o problemă pentru societățile dependente de o infrastructură sofisticată. Atacul fizic asupra unor centre critice pentru societate are efecte vizi-

bile. Dar pot exista și atacuri punctiforme asupra sistemelor infrastructurii critice, repetate și extinse pe parcursul unei perioade mai lungi de timp, fără un model exact și fără un autor imediat identificabil, care pot pune în pericol siguranța națională.

O problemă îngrijorătoare pe care o ridică o campanie susținută de atacuri asimetrice la adresa infrastructurii este *criza de încredere publică* ce poate rezulta. Se poate crea iluzia că instituțiile publice și cele private sunt incapabile de a asigura bunăstarea indivizilor.

Aceste lucruri nu sunt menite să descrie un viitor apocaliptic. Vor doar să sublinieze gravitatea provocării. Problema pe care o reprezintă protecția infrastructurii critice este aceea că în societățile dezvoltate din punct de vedere economic sectoarele public și privat sunt doar semi-compatibile. Acestea au scopuri diferite, motivații diferite, responsabilități diferite și „produse" diferite. Provocările pe care le ridică cooperarea dintre aceste sectoare se bazează pe trei aspecte: transmiterea informațiilor; aspecte legale; provocările tehnice.

Dificultățile *transmiterii informațiilor* își găsesc originea la nivelul percepțiilor și încrederii. De cele mai multe ori, sectoarele public și cel privat nu au încredere deplină unul în celălalt. În mod cert, companiile din cadrul aceluiași sector comercial al infrastructurii nu sunt caracterizate de o încredere reciprocă, în ciuda acordurilor de parteneriat. Există date confidențiale privind anumite proceduri și vulnerabilități. Pe de altă parte, guvernul, și în special sectorul de apărare și securitate națională, este interesat de informațiile clasificate, iar legile și regulamentele limitează transmiterea și diseminarea acestora.

Odată ce transmiterea informațiilor este considerată necesară, ce tipuri de informații trebuie să circule între sectorul public și cel privat, pe de-o parte, și în cadrul sectoarelor infrastructurii, pe de altă parte. Datele și analizele privind amenințările trebuie transmise. Dar ce se întâmplă cu datele și analizele privind vulnerabilitățile, care se desprind din cele dintâi? Acesta este un aspect foarte delicat.

Aspectele legale sunt și ele o problemă. În cadrul sectorului privat există preocupări pentru situații precum anti-trustul. Există apoi o serie de aspecte legale internaționale care depășesc aria de interes a unui stat-națiune.

Există, de asemenea, o serie de aspecte tehnice care complică procesul colaborării dintre sectoarele public și privat în protecția infrastructurii. Acest lucru se aplică mai ales în domeniul tehnologiei informaționale, iar procesele rezultante de „e-business" și „e-commerce" schimbă natura întregului sector privat. Pentru acesta din urmă, viteza afacerilor este principalul motor. Afacerile se dezvoltă și se adaptează azi mai rapid decât o va face vreodată guvernul.

Această dezvoltare rapidă este posibilă numai în absența intervenției guvernamentale. Inovația tehnologică provine aproape în exclusivitate din sectorul privat. Iată de ce problema colaborării public-privat în protecția infrastructurii critice se complică.

Societățile avansate se îndreaptă către o sferă nouă, indiferent că aceasta se numește sferă informațională sau ciber-spațiu. În acest demers, omenirea va aduce cu ea vechile ei nevoi și impulsuri: nevoia de a comunica, de a conversa, de a comercializa. Ea va aduce cu ea și impulsul către violență, conflict și război. Iar în procesul acestei migrări, se vor dezvolta și necesități, impulsuri și obiceiuri noi. Printre acestea se află și nevoia de protecție a infrastructurilor critice (fizică și informațională).

RĂZBOIUL INFORMAȚIONAL ȘI LEGISLAȚIA INTERNAȚIONALĂ

O problemă importantă asociată conceptului de război informațional este aceea potrivit căreia principiile legale ce guvernează acest spațiu sunt încă neclare.

Dezbaterile asupra problematicii războiului informațional au scos deseori în evidență problemele tehnologiei moderne, fără a lua însă în discuție mediul legal internațional actual.

Nu există acorduri internaționale care să se refere în mod special la controlul sau interdicția războiului informațional,

la fel de bine cum nu există legi al căror text să conţină explicit sintagma „război informaţional". Cât de mare este, în acest caz, decalajul dintre legislaţia internaţională şi toată problematica pe care o presupune războiul informaţional?

Examinarea relaţiei dintre războiul informaţional şi legislaţia internaţională presupune, inevitabil, explorarea câtorva probleme caracteristice: ce reprezintă „războiul" în epoca informaţională şi ce tipuri de activităţi pot fi numite „război informaţional"? Ce este un act de „război informaţional"? Ce devin „forţa", „atacul armat" sau „agresiunea armată" într-o eră a informaţiei? În ce mod sunt sau pot fi afectate noţiuni ca „suveranitatea naţională", „inviolabilitatea frontierelor"?

Războiul informaţional ridică câteva provocări importante legislaţiei internaţionale actuale.

În primul rând, legile internaţionale definesc starea de război şi starea de pace. Pentru a face această distincţie, nivelul şi natura pagubelor este un criteriu. Pagubele produse de atacurile informaţionale pot fi diferite de cele create de un război tradiţional. Pentru a lua un exemplu, distrugerile cauzate de bombe sunt uşor de observat, în vreme ce alterarea sau manipularea sistemelor informatice pot produce pagube intangibile, cum ar fi o perturbare a serviciilor de orice natură şi chiar a societăţii, în final. Acest lucru întăreşte convingerea că războiul informaţional este capabil să şteargă linia incertă, din punct de vedere filosofic, dintre război şi pace.

În al doilea rând, până în prezent, statele au constituit subiectul major al legislaţiei internaţionale. Statele sunt entităţi care posedă o autoritate suverană asupra unui anumit teritoriu. Însă posibilitatea semnalelor, de exemplu, de a traversa reţele internaţionale pune în discuţie conceptul de suveranitate teritorială naţională, principiu fundamental al relaţiilor internaţionale de la Tratatul de la Westfalia, din 1648, care stabileşte faptul că fiecare naţiune are o autoritate exclusivă asupra evenimentelor care se petrec în interiorul graniţelor sale.

Noutatea tehnologiilor ar putea explica absenţa oricărei măsuri de prevedere explicită în legislaţia internaţională care să interzică practicile ce ţin de fenomenul cunoscut sub denu-

mirea de „război informațional". Absența unor astfel de măsuri este importantă, căci, în general, ceea ce legislația internațională nu interzice, este permis. Pe de altă parte, inexistența acestora nu este hotărâtoare, deoarece chiar dacă legislația internațională nu se referă direct la anumite arme sau tehnologii, principiile sale generale pot fi aplicate și în cazul acestora.

Conform tratatelor internaționale și a cutumei, teritoriul statelor neutre este inviolabil de către forțele beligerante, în cazul unui conflict. Încălcarea frontierelor naționale, în legislația internațională actuală, se referă în special la acțiunile fizice realizate. Nu se știe, însă, dacă un atac realizat printr-o rețea care traversează un teritoriu neutru sau utilizează sateliți, calculatoare sau rețele aparținând unor state neutre are aceeași valoare juridică ca aceea a unei incursiuni a unor trupe înarmate.

Astfel de atacuri sunt dificil de încadrat, în momentul de față, de legislația internațională. Războiul, în accepția sa tradițională, presupune forțe înarmate și violență. Articolul 2 (4) al Cartei O.N.U. interzice amenințarea sau utilizarea forței împotriva integrității teritoriale și independenței politice a statelor. Însă un atac informațional reprezintă o „utilizare a forței"? Ce înseamnă „forță"? Aceasta, din perspectiva articolului 2 (4), este privită ca „forță armată. Din acest punct de vedere, ne putem întreba dacă un atac informațional este o „utilizare a armelor".

Carta O.N.U. conține două importante excepții de la regulă care permit utilizarea forței armate. Este vorba, în primul rând, de utilizarea forței având autorizația expresă a Consiliului de Securitate și, în al doilea rând, de utilizarea forței ca măsură de auto-apărare.

Capitolul VII al Cartei permite Consiliului de Securitate să autorizeze utilizarea forței de către state, în cadrul coalițiilor formate ad-hoc sau în cadrul organizațiilor regionale după ce s-a stabilit că este vorba de o „amenințare a păcii", de o „ruptură a păcii" sau de un „act de agresiune".

Întrebarea care apare natural este aceea dacă un atac informațional poate fi considerat o „amenințare a păcii", o

„ruptură a păcii" sau un „act de agresiune" având în vedere caracterul său diferit de cel al unui atac fizic.

Adunarea Generală a O.N.U. a definit „agresiunea" plecând de la o viziune tradiţională a războiului. Declaraţia defineşte „agresiunea" pe care Consiliul de Securitate este autorizat să o constate drept „utilizarea forţelor armate de către un stat împotriva suveranităţii, integrităţii teritoriale sau independenţei politice ale unui stat sau într-o cu totul altă manieră incompatibilă cu Carta ONU". Categoria armelor informaţionale ar putea fi acoperită de fraza: „(...) utilizarea oricărei arme împotriva teritoriului unui alt stat". Un atac informaţional având ca miză „suveranitatea, integritatea teritorială sau independenţa politică" ar putea fi considerat un „act de agresiune" care să determine Consiliul de Securitate să ia poziţie.

A doua excepţie de la regulă o constituie acceptarea utilizării forţei ca mijloc de auto-apărare. Articolul 51 al Cartei recunoaşte dreptul inerent la auto-apărare a statelor în caz de „atacuri armate". Sunt însă atacurile informaţionale „atacuri armate"?

Dificultatea caracterizării anumitor forme ale războiului informaţional ca elemente de „forţă", „război" sau „agresiune", din punct de vedere al dreptului internaţional, nu presupune implicit şi imposibilitatea instituţiilor internaţionale de a răspunde la astfel de fapte. Capitolul VII al Cartei O.N.U., de exemplu, acordă Consiliului de Securitate autoritatea şi responsabilitatea de a determina existenţa oricărei „ameninţări a păcii" sau a oricărui act de agresiune şi de a decide maniera de a răspunde la acestea. Din această perspectivă, multe dintre atacurile informaţionale ar putea fi considerate „ameninţări ale păcii" şi, în consecinţă, ar putea deveni subiecte ale deciziilor Consiliului de Securitate.

Încercările de revizuire a unor aspecte ale legislaţiei internaţionale, care să surprindă mai temeinic fenomenul războiului informaţional, se fac timid simţite. Federaţia rusă, de exemplu, caută să iniţieze un curent favorabil punerii la punct a unei legislaţii internaţionale în privinţa războiului informaţional În acest sens, Federaţia rusă a prezentat la a 53-a Sesiune a Adunării Generale un proiect de rezoluţie

privind *„Realizările spațiului informatizat și al telecomunicațiilor, în contextul securității internaționale"*. Proiectul de rezoluție invita statele membre O.N.U. să-și exprime un punct de vedere asupra utilizării tehnologiilor informatice în scopuri militare, asupra definiției conceptelor „arme informaționale" și „război informațional", asupra oportunității elaborării unor norme juridice internaționale privind utilizarea armelor informaționale, asupra necesității creării unui sistem internațional de monitorizare a amenințărilor legate de securitatea informatică și de sistemele de telecomunicații (a 53-a Sesiune a Adunării Generale, 08.09 — 18.12.1998, punctul 64 pe ordinea de zi: *„Menținerea securității internaționale: Prevenirea degradării violente a Statelor")*.

Societatea informațională, dincolo de beneficiile pe care le aduce cu sine, ridică importante probleme. Guvernele se confruntă cu probleme fundamentale cum ar fi cele care privesc modul în care se pot garanta valorile democratice într-o societate informațională. Frontiera dintre starea de pace și cea de război este tot mai greu de identificat. Unde începe și unde se termină pacea? Aceasta n-ar putea fi doar un război insesizabil?

Pentru moment există opinii numeroase și diferite privind necesitatea surprinderii la nivelul legislației internaționale a activităților informaționale și maniera în care acestea pot deveni subiecte ale dreptului internațional, fiecare dintre acestea fiind motivată de interesele proprii.

În ciuda acestei stări de fapt, nu se poate trece cu vederea faptul că noțiunea de „război", așa cum este ea definită de Carta O.N.U., tinde să devină o noțiune depășită de evenimentele timpului nostru. Carta nu evoluează în același ritm cu realitățile de azi și tinde să ofere tot mai greu o imagine adecvată a lumii actuale.

ABORDAREA CURENTĂ A CONCEPTULUI DE SECURITATE NAȚIONALĂ

Având în vedere derularea sistematică a operațiilor informaționale, concepțiile privind *securitatea națională* trebuie

să se schimbe, să se adapteze din mers la noile tipuri de amenințări — amenințări indirecte, non — militare din care fac parte în primul rând agresiunile informaționale.

Abordarea securității naționale se face astăzi din perspectivă sistemică. Securitatea este recunoscută ca fiind un concept multidimensional, multicâmp, așa încât, la clasicele sale dimensiuni, se mai adaugă una: dimensiunea informațională, câmpul informațional. Ca un comentariu, o posibilă tipologie a câmpurilor de securitate este următoarea: câmpuri conceptuale; psiho-sociologice; geopolitice, geografice; fizice; câmpuri informaționale (ale sistemelor de decizie și de informație).

Inevitabil, R.I. și operațiile informaționale pun problema abordării componentei informaționale într-un sistem național de securitate și a formulării unei *concepții de securitate informațională* la nivel național.

Prin ***securitate informațională*** se înțelege *„starea de protecție a necesităților de natură informațională ale individului, societății și statului, care să permită asigurarea satisfacerii acestora și evoluția lor progresivă, independent de prezența amenințărilor de natură informațională, interne și externe"*.

O *politică de securitate informațională* — ca parte componentă a politicii de securitate națională — apare drept consecință soluționarea contradicției dintre nivelul real existent și cel necesar *de protecție a cerințelor informaționale* ale individului, societății și ale statului însuși.

Totodată, trebuie proiectat *un sistem național al securității informaționale*, ca parte integrată a sistemului de securitate națională.

Obiectivele acestuia sunt: relevarea și prognozarea factorilor destabilizatori și a amenințărilor informaționale asupra intereselor naționale; realizarea complexului de măsuri operative și de lungă durată pentru preîntâmpinarea și înlăturarea lor; crearea și menținerea în stare de pregătire a forțelor și mijloacelor de asigurare a securității informaționale.

Strategia actuală de Securitate acoperă în mai mare măsură domeniul securității naționale decât au făcut-o versiu-

nile precedente. Principalul obiectiv al strategiei este protecția cetățenilor și asigurarea intereselor naționale definite ca: prosperitate națională și dezvoltare democratică a societății; suveranitate; integrare europeană și euro-atlantică.

Documentul identifică riscurile externe și interne și arată că principalele riscuri sunt nemilitare.

Tendința la ora actuală este orientată spre minimizarea rolului forțelor armate (se vorbește tot mai mult de reducerea efectivelor, de reorganizarea lor). Din perspectiva securității, diferențele dintre națiuni să măsoară azi prin modul în care fiecare știe să administreze și să controleze noile tipuri de amenințări, implicit amenințările informaționale.

Problema creării sistemului de asigurare a securității naționale și mai nou problema redimensionării acestui sistem ținând cont de aspectele informaționale, după opinia specialiștilor străini, presupune o abordare complexă a înfăptuirii politicilor în toate domeniile de activitate: economic, diplomatic, militar, politic, cultural, informațional, etc. Pentru a putea transpune în practică, această abordare teoretică este necesară o bază metodologică care să cuprindă concepții comune referitoare la securitatea națională, mai precis la securitatea informațională, la maniera de asigurare a acesteia.

În momentul de față *informația* trebuie percepută la adevărata ei valoare: ca *armă, factor de risc, instrument operațional, tehnologie.*

Cu toate acestea, la ora actuală, bătălia informațională (cu tot ce presupune ea: culegere de informații, protecția informațiilor, interzicerea accesului la informații, managementul informațional, transportul informațiilor) este cea care domină spectrul relațiilor internaționale, diminuând în mod direct domnia de altă dată a luptelor armate, unde armele de foc erau stăpâne ale câmpului de luptă.

Pe plan internațional se vorbește azi tot mai mult de sferă informațională, de principiul informării adecvate a statelor comunității mondiale, care presupune: dreptul fiecărui stat la securitate informațională; asigurarea în egală măsură a securității informaționale a tuturor membrilor; luarea în considerare a tuturor părților fără nici un fel de discriminare ș.a.

În ziua de azi, sistemul național de securitate ar trebui să ia în calcul conceptul de *agresiune informațională.*

CONCLUZII

Rapida evoluție a tehnologiei informației a dus la o schimbare de paradigmă privind natura conflictelor. Războiul informațional este acum o noțiune practică pentru multe națiuni. Costul necesar pentru obținerea de capacități credibile defensive privind R.I. este relativ scăzut, cu siguranță mult mai mic decât cel necesar pentru realizarea unei siguranțe naționale convenționale. Iată de ce capacitățile în domeniul R.I. sunt o alegere atractivă pentru un spectru larg de entități tradiționale sau moderne.

R.I. are la bază o strategie integratoare care recunoaște importanța și utilitatea informațiilor în comanda și controlul sistemului de siguranță națională și în implementarea strategiei de securitate națională.

R.I. exploatează oportunitățile și vulnerabilitățile inerente dependenței crescânde de informație, concentrându-se asupra sistemelor și tehnologiei informaționale.

R.I. nu este un fenomen cu care se confruntă doar țările evoluate. Structura actuală a sistemului internațional se îndreaptă spre o relație de interdependență statală tot mai accentuată, în care sunt angrenate atât statele dezvoltate, cât și cele mai puțin dezvoltate.

Modul de a înțelege și de a percepe fenomenul R.I. diferă de la o țară la alta, în funcție de realitățile proprii fiecăreia și de interesele pe care consideră că le poate promova cu ajutorul acestui instrument.

În primul rând, R.I. poate fi înțeles doar în cadrul întregului complex de schimbări. El nu influențează doar sectorul militar, ci întreaga societate și comunitate internațională.

Unul dintre efectele tehnologiei informaționale este crearea spațiului virtual, ca o nouă dimensiune în care poate fi dus războiul. Spațiul virtual are elemente de bază inseparabile: forțele armate, națiunea și comunitatea internațio-

nală. Toate nivelurile de comandă și control pot fi atacate și, în consecință, trebuie să fie apărate. La toate nivelurile, omul este cel care are puterea de decizie finală. Acest aspect face din conceptul de „influență" o opțiune și un pericol. Statele moderne se confruntă cu o dilemă.

Pe de-o parte, digitalizarea este un stadiu evolutiv firesc spre care tind societățile moderne și, pe de altă parte, aceste progrese creează noi și serioase vulnerabilități.

În al doilea rând, R.I. este o adevărată problemă. El pune sub semnul întrebării o serie întreagă de „vechi adevăruri". Nu există soluții ușoare. Un prim pas ar fi înțelegerea faptului că există riscuri. Un alt pas constă într-o evaluare atentă a vulnerabilităților. Tehnologia aduce multe foloase, dar și o mulțime de greutăți.

În al treilea rând, planificarea și ducerea unui R.I. strategic este, în orice caz, un proces complex în care, așa cum este cazul cu toate formele de război, informațiile și serviciile de informații sunt un factor-cheie pentru dezvoltarea și desfășurarea unor planuri și operațiuni efective de R.I., fie pentru dezvoltarea unor măsuri proprii de protecție a sistemelor militare, fie pentru realizarea unui sistem de degradare a capacităților acționale ale unui (in)amic.

Nu în ultimul rând, studiile de vulnerabilitate, analizele efectuate pentru caracterizarea amenințării, simpozioanele internaționale dovedesc importanța acordată de comunitățile de informații acestui nou fenomen. Deja amenințarea informațională nu mai este doar problema specialiștilor din domeniul militar. Mass-media începe să propage efecte devastatoare ale acestei arme noi prea puțin convenționale.

R.I. a acordat, de altfel, un plus de autoritate actorilor și aspectelor netradiționale. Organizațiile mici cu buget restrâns sunt acum capabile de o mai mare agresivitate și influență decât ar fi putut prezice teoriile relațiilor internaționale. Din acest motiv, conceptul tradițional de siguranță națională trebuie să evolueze spre ceva mai flexibil, mai proactiv și mai dinamic. Pregătirea trebuie să vizeze cel puțin trei niveluri: *politic* — să se aibă imaginea de ansamblu a amenințărilor la adresa infrastructurii informaționale la nivel național și

internațional; *de intelligence* — să se înțeleagă indicatorii și avertizările și să se poată conlucra cu planificatorii strategici; *de sistem* — să se recunoască atacurile și să se știe cum să se reacționeze.

O *politică de securitate informațională* — ca parte componentă a politicii de securitate națională — apare drept consecință a soluționării contradicției adânci dintre nivelul real existent și cel necesar *de protecție a cerințelor informaționale* ale individului, societății și ale statului însuși.

Securitatea informațională este doar o componentă a strategiei complexe de securitate la nivel național, care este obligată să dispună în orice moment de toate pârghiile necesare.

Fără o înțelegere cât mai exactă, a ceea ce este și ceea ce nu este R.I., a ceea ce poate sau nu poate să rezolve, ca parte integrantă a politicii statului, nu se poate vorbi despre o viziune clar formulată, de adaptare a României la realitatea „transformărilor informaționale".

BIBLIOGRAFIE

Strategia de Securitate Națională a României, „Monitorul Oficial" nr. 822/20.12.2000;

Alvin și Heidi Toffler, *Război și Anti-Război*, Editura Antet, 1995

Neil Munro, *Inițiativele americane în domeniul R.I.*, Defense News, p.25–31;

Vasile Păun, Anca Monica Popa, *O provocare strategică-Războiul Informațional*, București:Editura UTI,2002;

Patrick Kleinknecht, *La guerre de l'information: un concept „fourre-tout"*, l'Armement nr. 60, dec. 1997/ian. 1998;

Martin Libicki, *What is information Warfare ?*, Institute for National Strategic Studies, ACIS Paper 3, aug. 1995, cap. 2;

Cornerstones of Information Warfare, 1995. Pentru alte definiții date R.I.: Rona Thomas, Richard D., *Special Report on I.W.*, Computer Security Journal, vol.11, nr. 2, 1996;

Martin Libicki, *Dominant Battlespace Knowledge: The Winning Age*, National Defense University Press, 1995 etc.;

Felix Faucon, *Guerre de l'information ou opérations d'information?*, Défense Nationale, an 54, nr. 3, martie 1998;

Manisov, *Sistemul de securitate națională: experiența unor state străine*, Zarubeznoe Voennoe Obozrenie, Rusia, nr. 10, 1995, p. 2–11.

DEMOCRAȚIA — RESURSĂ FUNDAMENTALĂ A MEDIULUI INTERN DE SECURITATE

Robert Veress

Este democrația o resursă fundamentală a mediului intern de securitate? Se poate vorbi de securitate socială, de securitate în general, în lipsa democrației? Răspunsurile sunt oferite chiar de definiția democrației.

Conform *Dicționarului Enciclopedic* (vol. II, Editura Enciclopedică, București, 1996), democrația este o „Formă de guvernare a unei societăți, bazată pe principiul participării poporului la conducere". În societatea modernă, poporul nu participă direct la guvernare, ci prin reprezentanți aleși. Principiile pe care se bazează democrația sunt: parlament reprezentativ, separația puterilor în stat, domnia legii (în opoziție cu domnia forței), garantarea drepturilor civile, proporție optimă între democrația orizontală (principiul participării generale la conducere) și democrația verticală (principiul ierarhiei).

Conform *Microsoft Encarta Encyclopedia Deluxe 2004*, democrația implică faptul că reprezentanții aleși sunt responsabili în fața electoratului și pot fi înlăturați în urma unui referendum. Aceasta înseamnă că aleșii ar trebui să decidă ținând cont de voința populară (a majorității). Encarta enunță și câteva dintre drepturile civile pe care le garantează democrația: proprietatea, egalitatea în fața legii, dreptul la educație, dreptul de a alege și de a fi ales, libertatea individuală, respectiv libertatea și responsabilitatea alegerii carierei și a conducerii propriilor afaceri.

Se poate lesne trage concluzia că absența democrației generează, automat, probleme de securitate, lucru demonstrat de istorie, de evoluția omenirii. Alte forme de guvernare, care nu asigură dreptul de vot și celelalte drepturi civile, separația puterilor și domnia legii, presupun o formă sau alta de dictatură. Anumite situații, în special unele de criză (ex.: foamete generată de calamități naturale), pot fi și chiar sunt mai ușor depășite de regimurile dictatoriale, despotice. Un despot „luminat" poate impune mult mai ușor deciziile nepopulare

care se dovedesc, ulterior, a fi soluțiile optime. Exemplele în acest sens abundă, în istorie. Însă, dictatura conduce, mai devreme sau mai târziu, la genocid.

Se spune despre Nicolae Ceaușescu că ar fi fost adulat, că i s-ar fi ridicat statui, păstrându-și prima pagină în manualele de istorie, dacă „s-ar fi oprit la timp". Adică, dacă înceta înfometarea poporului, după achitarea datoriilor externe. Dar Ceaușescu n-a fost, nici măcar în anii '60, un despot luminat. Altfel, succesele politicii sale externe din acei ani nu ar fi construit eșafodul „spânzurătorii" sale, declanșându-i paranoia. Alegând disidența față de soviete, un lider înțelept ar fi acționat în cunoștință de cauză, asumându-și riscurile. Ceaușescu s-a lăsat mânat de orgoliul său, care îi dădea ghes să se afirme ca unul dintre cei mai importanți oameni ai planetei. Orgoliul a fost mai puternic decât instinctul de conservare, instinct care i-a împiedicat pe conducătorii celorlalte state-satelit ale USSR să le dea cu tifla liderilor de la Kremlin. În momentul în care Ceaușescu a constatat că este pe lista neagră a Moscovei, instinctul de conservare a preluat „conducerea", iar cizmarului i s-a făcut frică. Frica a rămas, dar a crescut și orgoliul, alimentat de constatarea scăpării de la mazilire. A rezultat un amestec exploziv, care a distrus viețile mai multor generații.

Paradoxal, imperfecțiunile democrației țin, într-o mare măsură, tocmai de ceea ce o apropie de forma de guvernare ideală (nedescoperită), anume de libertățile individuale. Abuzul de libertate generează probleme, uneori dintre cele mai grave, primejduind securitatea mediului intern și chiar pe a celui extern. Abuzul de libertate se poate dovedi chiar mai primejdios decât reprimarea libertăților. Aceasta poate fi o cauză (nu obligatorie, dar posibil obiectivă) a pendulării unor state între cele două forme de guvernare: democrație și dictatură. De fapt, perioadele de democrație autentică sunt destul de scurte, iar în majoritatea statelor care se laudă cu un regim democratic, funcționează un simulacru de democrație. O situație oarecum aparte se înregistrează în Statele Unite, care au limitat, temporar, anumite libertăți individuale, fiind angrenate în războiul împotriva terorismului. În acest caz, se poate vorbi de o suspendare a democrației, în scopul prezervării acesteia.

DEMOCRAȚIA ORIGINALĂ

Scăpată de dictatura iataganului, România a devenit, treptat, un stat democratic (monarhie constituțională). Apoi, a revenit la dictatură, care a îmbrăcat diverse forme: legionară, regală, antonesciană, comunistă. Sfârșitul anului 1989 a adus izbăvirea de comunism și o reinstaurare a democrației — a unei forme primitive de democrație, în care abuzul de libertate este la ordinea zilei, la toate nivelurile. Nu întâmplător sunt atâția nostalgici ai perioadei ceaușiste, în care viața părea mai simplă, mai sigură. Este România un stat democratic? Răspunsul, venind din partea unui patriot adevărat, deci obiectiv, ar fi „da", dar un da anemic, fără litere mari și fără semnul exclamării. Răspunsul pozitiv vizează principialul: România are fundamentele democrației — o Constituție democratică, alegeri libere, libertate de exprimare.

Dar, democrația, în România anului de grație 2004, nu este (încă) funcțională, punerea în practică a principiilor constituționale lasă mult de dorit. Cauza principală a respectivei stări de fapt este cvasi-cunoscută: corupția generalizată. Acest flagel, a transformat țara noastră într-un stat asocial, în care majoritatea cetățenilor nu se mai gândesc decât la propriul interes, neglijându-și complet sau într-o foarte mare măsură rolul în societate, obligațiile față de aceasta.

Chiar dacă am depășit perioadele cele mai dificile, consemnate în anii 1997–1999, când disoluția autorității statului împinsese România în pragul anarhiei, suntem departe de o situație liniștitoare, în care grosul populației să cunoască și să respecte regulile „jocului" democratic. Starea de insecuritate, pe care o resimt foarte mulți cetățeni, este cauzată tocmai de punctele slabe ale democrației românești, plastic botezată ca fiind „originală". Atunci când foarte mulți cetățeni (de ordinul sutelor de mii sau chiar al milioanelor) nu se simt în siguranță, însăși securitatea națională și funcționarea statului de drept sunt amenințate.

Astfel, misiunea celor chemați să asigure „mediul intern de securitate" este să apere, mai presus de orice, democrația. Iar dacă inamicul nr.1 al democrației este corupția, atunci priori-

tatea de acțiune, în sensul prezervării și întăririi securității interne, este combaterea corupției. Este fără echivoc faptul că mass-media, jurnaliștii joacă un rol capital în demascarea faptelor de corupție. În acest fel (și în altele), presa este în avanposturile luptei pentru democrație, pentru securitatea națională. O luptă dură, care, iată, face victime printre ziariști. Fără ca, din păcate, autorii agresiunilor împotriva jurnaliștilor să fie identificați și trași la răspundere de către cei în drept.

SUSPENDAREA DEMOCRAȚIEI

După atentatele din 11 septembrie 2001, mii de persoane, a căror identitate nu a fost dezvăluită, au fost arestate și aruncate în închisori civile și militare din Statele Unite. Aparent, singura lor vină a fost apartenența spirituală la Islam, fiind musulmani cu cetățenie americană sau cu altă cetățenie. Într-un fel, situația de acum e comparabilă cu cea din anii '40–'70, din a doua jumătate a directoratului Hoover la FBI, când a fost practicată „vânătoarea de vrăjitoare" împotriva celor bănuiți de activități comuniste. În decursul celebrei operațiuni — secretă la vremea ei — COINTELPRO, lansată în 1956, și al altora asemănătoare, FBI a acționat împotriva celor bănuiți de activități subversive la adresa SUA, dar și a militanților pentru drepturile civile, în special împotriva persoanelor de culoare. Agenții FBI au pătruns ilegal (fără mandat) în casele oamenilor, le-au ascultat convorbirile telefonice, au folosit informațiile astfel obținute în scop de șantaj. Șantajul a devenit arma prin care Hoover a ajuns, practic, să controleze clasa politică și să-și protejeze, astfel, poziția, abuzând deschis de aceasta, în scopul obținerii unor foloase materiale. Este greu de imaginat cum ar fi arătat America, astăzi, dacă Hoover ar mai fi trăit măcar 5 de ani. Ar mai fi existat, oare, scandalul Watergate, care a dus la demisia președintelui Nixon?

Cu toate abuzurile de acum, este greu de imaginat că acestea se vor permanentiza, că nivelul la care a evoluat democrația americană nu va atârna suficient în balanța democrație

versus dictatură. Iată, chiar dacă mai lent decât în cazurile civile, procedurile juridice au evoluat și în cazul presupușilor membri Al-Qaeda încarcerați la baza Guantanamo, astfel că a început eliberarea acelora împotriva cărora nu s-au putut prezenta dovezi incriminatorii consistente. Putem vorbi, totuși, de o suspendare a democrației americane, așa cum arăta ea la hotarul dintre milenii, de o încălcare a Principiilor de la Johannesburg.

Dacă, așa cum am arătat, în SUA există suficiente și eficiente mecanisme de reglare a derapajelor spre dictatură, nu la fel stau lucrurile în statele cu democrații incipiente sau insuficient evoluate. Din acest punct de vedere, adoptarea, în SUA, a unor legi de tipul USA Patriot Act, din 2001, poate avea consecințe nefaste pentru democrația globală. Implicit, pentru securitatea globală. Nimeni nu poate pretinde că în lupta împotriva terorismului trebuie acționat cu mănuși. Dar, în goana după securitate națională și globală, SUA se aseamănă cu un atlet care se dopează, tocmai din cauza suspendării unor libertăți democratice și a modului imperialist de acțiune, manifestat atât de vizibil prin modalitatea de „gestionare" a crizei irakiene. SUA interpretează original concepția lui F. Fukuyama, pentru care valorile democratice devin instrumentul de cucerire a spatiilor noi.

PARADOXUL CHINEZESC

Ce este China de azi? Evident, nu este o democrație, nici măcar una „populară", așa cum pretind liderii de la Beijing. Dar nici nu se mai poate vorbi de o dictatură în sensul deplin al cuvântului, câtă vreme acolo există economie de piață. De vreme ce standardul de viață este în creștere în țara Fluviului Galben — evoluție atipică pentru un stat comunist —, ar fi interesant de știut ce s-ar întâmpla dacă s-ar organiza alegeri libere în China, cât de bine ar reuși să se plaseze comuniștii în preferințele electorilor.

Cum ar arăta o Chină reformată politic, democratizată? Ar fi bine pentru mediul intern de securitate al Chinei, dacă țara ar schimba stindardul roșu cu unul multicolor? Ar putea

suporta lumea o Chină democratică? Dacă e să ne luăm după evoluția relațiilor chino-americane din ultimii 15 ani și după evoluția PC chinez în aceeași perioadă, putem conchide că analiștii CIA au decis că răspunsul la ultima întrebare este negativ. Cel puțin dacă prin „lume" se înțelege America. În principiu, un răspuns negativ la a treia întrebare implică un răspuns negativ la întrebarea a doua, vizând mediul intern de securitate. Pentru că logic ar fi ca o Chină stabilă, cu un mediu intern de securitate sănătos, să nu prezinte un pericol pentru securitatea globală. Se poate, desigur, invoca pericolul migrației, dar mecanismele de blocare sau restrângere a acesteia nu trebuie să fie neapărat interne.

Așadar, dacă analiștii CIA nu s-au înșelat, apare posibil ca democrația să nu fie, întotdeauna, o resursă fundamentală a mediului intern de securitate, ci, dimpotrivă, să genereze insecuritate. Un paradox, o contradicție aparentă cu cele afirmate în deschiderea lucrării. De fapt, nu democrația, în sine, ar putea genera insecuritate în China, ci, eventual, apariția ei abruptă, după „modelul românesc". Să recunoaștem, o Chină ca o Românie în tranziție aparent perpetuă, multiplicată de câteva zeci de ori, ar însemna dezastru planetar. E de preferat o tranziție, chiar neasumată ca atare, spre o societate modernă, patronată de comuniștii reformați, care continuă să aplice pedeapsa capitală pentru corupție.

BIBLIOGRAFIE

Dicționarul Enciclopedic, vol. II, Editura Enciclopedică, București, 1996.

Microsoft Encarta Encyclopedia Deluxe, 2004.

Studii de securitate, vol.1, 2003.

Principiile de la Johannesburg privind siguranța națională, libertatea de exprimare si accesul la *informație*, 1octombrie 1995).

USA Patriot Act, *2001, cu comentariile prof. John Podesta, copreședinte al Centrului pentru Studii* Legale al Universității Georgetown

SECURITATEA ALIMENTARĂ COMPONENTĂ A SECURITĂȚII NAȚIONALE

Narcisa Georgescu

Alimentația constituie una din cele mai importante necesități fiziologice ale omului. Elementele privind necesarul organismului în substanțe nutritive și interacțiunea dintre ele sunt sintetizate în teoria alimentației echilibrate. Conform acestei teorii, pentru o bună asimilare a hranei și o funcționare optimă a organismului este necesară aprovizionarea acestuia cu toate substanțele nutritive în proporții bine stabilite.

Politica alimentară a Uniunii Europene și României trebuie construită pe baza standardelor de siguranță alimentară care servesc la protejarea și promovarea sănătății consumatorului. Producția și consumul de alimente sunt elemente centrale în orice societate și au consecințe economice, sociale și în multe cazuri, asupra mediului.

Cu toate că protecția sănătății trebuie să aibă întotdeauna prioritate, în dezvoltarea politicilor alimentare trebuie de asemenea să fie luate în considerare aceste aspecte. În plus, condiția și calitatea mediului, în special al ecosistemului pot afecta diferitele stadii ale lanțului alimentar. Principiul de bază al siguranței alimentare este ca aceasta să se bazeze pe o abordare cuprinzătoare, integrată. Aceasta presupune parcurgerea întregului lanț alimentar, „de la ferma pe masă".

O politică eficientă de siguranță alimentară trebuie să recunoască natura interconexiunilor din cadrul producției alimentare. Aceasta necesită evaluarea și monitorizarea riscurilor asupra sănătății consumatorului, asociate cu materiile prime, practicile agricole și activitățile de prelucrare alimentară, necesită acțiuni eficiente de reglementare pentru a controla acest risc și înființarea și operarea sistemelor de control pentru a monitoriza și aplica operarea acestor reglementări.

Este necesară o mai bună coordonare și integrare a siguranței alimentare. Aceasta va permite abordarea punctelor

slabe existente, creând în același timp un cadru real de siguranță alimentară, care poate asigura un nivel ridicat al sănătății publice și protecției consumatorului.

CONCEPTUL DE SECURITATE ALIMENTARĂ

Securitatea alimentară este definită ca fiind „accesul pentru toată lumea și în mod permanent la hrana necesară unei vieți active și sănătoase". Nivelul la care este evaluată securitatea alimentară poate fi cel global (mondial), regional, național, familiar și individual.

Accepțiunea generală este aceea că insecuritatea alimentară și foamea sunt în mod direct rezultatul sărăciei. Odată cu creșterea economică și mărirea veniturilor, familiile sărace vor avea abilitatea și dorința de a obține o dietă adecvată, cel puțin în termeni energetici.

O altă problemă ce trebuie abordată se referă la raportul dintre securitatea alimentară și asistența alimentară. Asistența alimentară este definită ca ansamblul inițiativelor luate de guvern, adesea în colaborare cu organizațiile neguvernamentale și membrii societății civile și, atunci când este necesar, cu ajutor extern, pentru ameliorarea necesarului de alimente a cetățenilor lor care, fără acestea, nu ar avea acces la hrană suficientă pentru o viață sănătoasă și activă.

Foamea locală este o problemă mondială. Dreptul fiecăruia la hrană a fost enunțat în numeroase declarații și pacte ale Națiunilor Unite. Ca urmare, din considerații umanitare funadamentale, comunitatea internațională își aduce aportul prin ajutor alimentar, pentru a sprijini combaterea foamei.

Pot fi formulate și câteva principii ale securității alimentare. Bunăoară, *principiul coordonator* se referă la faptul că politica de securitate alimentară trebuie să se bazeze pe o abordare cuprinzătoare, integrată. Aceasta presupune parcurgerea întregului lanț alimentar (de la fermă pe masă), trecând prin toate sectoarele alimentare, între România și celelalte state, la frontiera externă a României și în interiorul acesteia,

la nivelul forurilor de decizie și în toate stadiile ciclului de elaborare a politicii. Principiile fundamentale ale siguranței alimentare (consultanța științifică, colectarea și analiza datelor, aspecte de reglementare și control și de informare a consumatorului) trebuie să formeze un întreg uniform pentru a se realiza această abordare integrată.

Trebuie definite clar rolurile tuturor celor implicați în lanțul alimentar, respectiv fabricanții de alimente, fermierii și producătorii agricoli, operatorii alimentari, autoritățile competente și nu în ultimul rând consumatorul, *responsabilitatea* primară pentru siguranța alimentară revine producătorilor de alimente, fermierilor și operatorilor, iar monitorizarea și aplicarea acestei responsabilități primare revine autorităților competente prin sistemele naționale de supraveghere și control.

Consumatorii trebuie să accepte să sunt responsabili pentru depozitarea, manipularea și pregătirea corespunzătoare a alimentelor în gospodăriile proprii, astfel încât principiul responsabilității va cuprinde toate sectoarele lanțului alimentar „de la fermă pe masă".

O politică alimentară de succes presupune identificarea furajelor și alimentelor și a ingredientelor acestora. Producătorii de furaje și de alimente au obligația să asigure aplicarea procedurilor adecvate de retragere a furajelor și alimentelor de pe piață, atunci când este identificat un risc pentru sănătatea consumatorilor. Operatorii trebuie de asemenea să țină evidențe ale furnizorilor de materii prime și ingrediente pentru a permite identificarea sursei problemei.

Abordarea cuprinzătoare și integrată va conduce la o politică alimentară mai *coerentă, eficientă și dinamică.* Politica trebuie revizuită constant și la nevoie, să fie adaptată pentru a răspunde lipsurilor, pentru a face față riscurilor ce apar și pentru a recunoaște noile tendințe din cadrul lanțului de producție. În același timp, dezvoltarea acestei abordări trebuie să fie transparentă, implicându-i pe toți cei interesați și permițându-le să aducă contribuții efective la noile tendințe.

Analiza riscului trebuie să constituie fundamentul pe care să se bazeze politica de siguranță alimentară. România tre-

buie să-și bazeze politica alimentară pe aplicarea a trei componente ale analizei riscului: evaluarea riscului (consultanță științifică și analiza informațiilor), managementul riscului (reglementare și control) și comunicarea riscului. De asemenea, România va continua să utilizeze cele mai bune metode științifice disponibile în elaborarea măsurilor de siguranță alimentară.

Organizarea consultanței științifice independente și asumarea faptului că atât consumatorii cât și industria alimentară trebuie să aibă încredere că această consultanță este furnizată la cele mai ridicate standarde de independență, excelentă și transparentă.

ELEMENTE ESENȚIALE ALE POLITICII DE SECURITATE ALIMENTARĂ

Colectarea și analiza informațiilor sunt elemente esențiale ale politicii de securitate alimentară și sunt importante în special pentru identificarea riscurilor potențiale asupra alimentelor și furajelor. Dintre elementele esențiale ale politicii de securitate alimentară putem face referire la următoarele:

Monitorizarea și supravegherea. Există un volum mare de informații privind aspectele de siguranță alimentară. Sursele principale de informare sunt rețelele de monitorizare și supraveghere a sănătății publice, planuri de supraveghere a zoonozelor și reziduurilor, sisteme de alertă rapidă, sisteme de informare în sectorul agricol și cele de cercetare. Primul obiectiv trebuie să fie un management continuu și zilnic al informației pentru a permite un răspuns real, la timp, față de riscurile potențiale.

Sisteme de alertă. În general, sistemul de alertă rapidă pentru alimente funcționează bine pentru produsele alimentare destinate consumatorului final. Există diferite alte tipuri de sisteme de avertizare în diferite domenii, cum ar fi bolile transmisibile la oameni și animale, produsele animaliere

stopate la graniță, transportarea animalelor vii și sistemul ECURIE în caz de urgență radiologică.

Cercetarea. Un nivel de excelență științifică necesită investiții în cercetare și dezvoltare pentru a extinde baza de cunoștințe științifice privind siguranța alimentară. Cercetarea și dezvoltarea trebuie să se desfășoare pe baza unor programe de lucru multianuale, ale căror obiective să fie orientate spre rezolvarea problemelor, în principal cele privind cetățenii și nevoile acestora. Activitățile de cercetare trebuie să se desfășoare în special în domeniul tehnologiilor alimentare avansate, privind metodele mai sigure de producție și distribuție a alimentelor, noile metode de evaluare a riscurilor chimice și expunerilor la contaminare, rolul alimentelor în promovarea sănătății.

Cooperarea științifică. La nivelul Europei informațiile științifice sunt compilate de instituții și organizații naționale privind o gamă largă de subiecte referitoare la siguranța alimentară, în cadrul sistemului de cooperare științifică. Numai într-un număr limitat de domenii s-a stabilit coordonarea informației științifice pentru a se construi o imagine europeană, iar în multe cazuri nu pot fi furnizate informațiile necesare pentru o evaluare a riscurilor la nivel european, motiv pentru care este necesară o cooperare științifică între țările europene.

Consultanța științifică. Politica de siguranță alimentară are la bază informațiile științifice drept urmare, consultanța științifică privind siguranța alimentară trebuie să fie de cea mai bună calitate și furnizată la timp și corect celor responsabili de luarea deciziilor privind protecția sănătății consumatorului. Este necesară reorganizarea Sistemului de acordare a consultanței științifice, punându-se accent pe principiile fundamentale de excelență, transparență și independență. De asemenea, este necesară reorganizarea comitetelor științifice sectoriale care să acorde consultanță în domenii multidisciplinare, cum ar fi BSE (encefalopatia spongiformă), rezistența anti-microbiană, contaminarea radioactivă a alimentelor și furajelor etc.

RESPONSABILITĂȚI SPECIFICE LEGATE DE EVALUAREA RISCULUI ȘI COMUNICAREA PRIVIND ASPECTELE DE SECURITATE ALIMENTARĂ

O prioritate de bază a autorităților este să ia măsuri eficiente pentru a asigura un nivel ridicat al protecției consumatorului, prin care să se restabilească și să se mențină încrederea acestuia. Rolul autorităților trebuie definit în contextul procesului de analiză a riscului, care cuprinde evaluarea, managementul și comunicarea riscului.

Obiectivul evaluării riscului este acordarea de consultanță științifică. Rețelele de monitorizare și supraveghere în domeniul sănătății publice și animale, sistemele de informare în sectorul agricol și sistemele de alertă rapidă, cât și programele de cercetare și dezvoltare, joacă un rol important în elaborarea cunoștințelor științifice.

Legislația și controlul sunt cele două componente ale *managementului riscului.* Legislația implică o decizie politică și aprecieri care să se bazeze nu numai pe știință, ci și pe o apreciere a dorințelor și nevoilor societății. În perspectiva aderării la Uniunea Europeană, autoritățile sunt responsabile de asigurarea transpunerii corecte a legislației comunitare în cea națională și de implementare și aplicare corectă a acesteia.

Funcția de control este realizată de organismele autorității de control, rapoartele acestora privind constatările și recomandările reprezintă elemente de bază în deciziile privind luarea măsurilor de siguranță alimentară. Funcția de control trebuie să ofere un nivel ridicat de responsabilitate și transparență și să se afle în centrul procesului de management al riscului privind siguranța alimentară.

Comunicarea riscului este un element de bază în asigurarea unei informări continue a consumatorilor și în reducerea riscului problemelor nedorite de siguranță alimentară care apar. Responsabilitățile autorităților constau în pregătirea și acordarea de consultanță științifică, colectarea și

analiza informațiilor necesare pe care se fundamentează, atât procesul de consultanță, cât și cel de luare a deciziilor, monitorizarea și supravegherea problemelor de siguranță alimentară și comunicarea constatărilor sale către terțe părți.

Autoritățile trebuie să colaboreze îndeaproape cu agențiile și instituțiile științifice naționale responsabile de siguranța alimentară. Obiectivul principal al autorităților este să contribuie la sprijinirea protecției sănătății consumatorului în domeniul siguranței alimentare, prin care se poate restabili și menține încrederea consumatorului.

NOUL CADRU LEGISLATIV PENTRU SIGURANȚA ALIMENTARĂ

Noul cadru legislativ trebuie să stabilească principiile pentru asigurarea unei abordări coerente și să definească principiile, obligațiile și definițiile care se aplică în acest domeniu.

Este necesară o *Lege generală a alimentului*, care va materializa principiile siguranței alimentare. Propunerile privind această lege trebuie să facă subiectul consultării complete cu toate grupurile interesate. Legislația individuală trebuie să fie clară, simplă și inteligibilă pentru ca toți operatorii să o poată aplica. Există de asemenea, nevoia unei strânse cooperări cu autoritățile competente la nivelele corespunzătoare, pentru a asigura respectarea și aplicarea corectă și armonioasă și pentru a evita procedurile administrative inutile.

SĂNĂTATEA ȘI BUNĂSTAREA ANIMALELOR

Sănătatea și bunăstarea animalelor din care se produc alimente este esențială pentru sănătatea publică și protecția consumatorului. Sănătatea animală este de asemenea un factor important în siguranța alimentară. Anumite boli, așa numitele zoonoze, cum ar fi tuberculoza, salmoneloza și listerioza se pot transmite la oameni prin alimentele contaminate.

Aceste boli pot fi deosebit de periculoase pentru anumite categorii ale populației.

Programele existente de eradicare și control al bolilor, trebuie continuate și întărite pe cât posibil, în special în acele state al căror statut cu privire la aceste boli rămâne problematic.

Legislația trebuie să prevadă în special promovarea sănătății și bunăstării animalelor, numai în măsura în care este implicată direct politica de siguranță alimentară. Se recunoaște necesitatea integrării mai complete a aspectelor de bunăstare animală în politica alimentară. În special, legislația trebuie să respecte impactul privind calitatea și siguranța produselor de origine animală destinate nevoilor consumului uman.

DREPTURILE FUNDAMENTALE ALE CETĂȚENILOR ȘI ACTIVITATEA DE SIGURANȚĂ NAȚIONALĂ

Marian Dumitrescu

„România este stat de drept, democratic și social, în care demnitatea omului, drepturile și libertățile cetățenilor (...) reprezintă valori supreme și sunt garantate".

Art.1, alin.3 din Constituția României

Problematica drepturilor omului, a libertăților fundamentale și activitatea de siguranță națională este deosebit de actuală și importantă, deoarece o serie de definiții rezulate din corelarea celor două dimensiuni nu și-au găsit răspunsuri pertinente și consensuale.

Schimbările politice, sociale și economice determinate de evenimentele lui decembrie 1989 au modificat radical modul de percepere a acestor două concepte. România a trecut de la totalitarism la democrație; statul totalitar este înlocuit cu statul de drept: cetățeanul este acum totul. Alături de asigurarea principiilor separării puterilor, asumării sarcinii de realizare a unei societăți mai integrată, mai echilibrată, statul de drept are ca principal deziderat asigurarea și respectarea drepturilor fundamentale ale omului, ale cetățeanului.

Rațiunea de a fi a serviciilor de siguranță națională o constituie chiar cetățeanul, cu ale sale drepturi, libertăți și îndatoriri fundamentale. Serviciile de siguranță există acum într-un cadru legal, democratic în concordanță cu reglementările intenaționale referitoare la drepturile omului. Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Protecție și Pază, structurile specializate ale Ministerului de Interne, Ministerului Apărării Naționale, Ministerului de Justiție sunt organe expres prevăzute de Legea Siguranței Naționale, funcționând în baza unor legi organice.

Cadrul legislativ este clar structurat în acest domeniu, nepermițând nici o violare arbitrară a drepturilor cetățeanului.

SISTEMUL DE DREPT UMANITAR INTERNAȚIONAL

Cinci acte constitutive ale O.N.U. și ale unor instituții specializate: Carta O.N.U., Constituția O.I.M., Convenția UNESCO, Constituția E.A.O. tratează problematica drepturilor omului, instituționalizând principiile de bază ale acesteia, iar alte cinci instrumente juridice, Declarația Universală a Drepturilor Omului, Pactul Internațional referitor la drepturile economice, sociale și culturale, Pactul Internațional cu privire la drepturile civile și politice și cele două protocoale adiționale la acestea din urmă, denumite generic Carta internațională a drepturilor omului, reglementează aspectele globale ale problematicii drepturilor omului. Alte multe instrumente internaționale, adoptate sub auspiciile forului internațional, acoperă diverse domenii: în planul drepturilor civile și politice. Au fost elaborate acte normative referitoare la dreptul la autodeterminare, dreptul la viață, abolirea sclaviei, a muncii forțate, a comerțului cu ființe umane, protecția persoanelor supuse detenției sau întemnițării, ameliorarea situației refugiaților, libertatea de opinie și exprimare, libertatea de asociere, protecția minorităților etc. În planul drepturilor economice sociale și culturale, domeniile reglementate privesc dreptul la muncă, la educație, la sănătate, la hrană etc. Alături de acțiunea statelor membre ale comunității internaționale, concentrată în sistemul O.N.U., de definire a drepturilor omului pentru a căror aplicare să acționeze apoi pe plan intern, după crearea Națiunilor Unite s-au înregistrat preocupări de reglementare diferențiată, în plan regional, a drepturilor, libertăților și îndatoririlor constatându-se tratarea și detalierea de o manieră aparte. Astfel, pe plan european, în cadrul O.S.C.E. au fost adoptate acte, cum ar fi Actul final de al Helsinki din 1975, Documentul de la Viena din 1986, Carta de la Paris din 1990, Declarația de la Copenhaga din 1992, Tratatul de la Nisa din 2000, în care problematica

drepturilor omului este amplu reglementată. În cadrul subregional, a fost adoptată de către Consiliul Europei, de la 4 noiembrie 1950, Convenția pentru protecția drepturilor omului și libertăților fundamentale.

În 1952, Adunarea Generală a recomandat elaborarea a două pacte internaționale — unul pentru drepturile civile și politice și altul pentru drepturile economice, sociale și culturale. La 16 decembrie 1966, Adunarea Generală a O.N.U. a adoptat următoarele trei instrumente: „Pactul internațional privitor la drepturile economice, sociale și culturale", Pactul internațional privitor la drepturile civile și politice, Protocolul facultativ la acest ultim pact, care prevede un mecanism de examinare a plângerilor persoanelor particulare. Pactul internațional cu privire la drepturile economice, sociale și culturale a intrat în vigoare la 3 ianuarie 1976, iar Pactul internațional referitor la drepturile civile și politice și Protocolul facultativ, la 25 martie 1986.

Constituția României adoptă prin referendum a receptat trăsăturile fundamentale ale libertăților publice protejate prin instrumente juridice internaționale.

SERVICIILE DE INFORMAȚII ȘI RESPECTAREA DREPTURILOR OMULUI

Serviciile de siguranță națională sunt acele organe ale administrației publice[120] ce au ca scop *cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe ce pot aduce atingere valorilor* menționate mai sus (art.2, alin.1 din Legea nr. 51/1991). *Amenințarea este starea pericolului potențial, a cărui realizare materială devine posibilă, probabilă, iminentă sau consumată, în funcție de o serie de factori ulteriori, iar amenințarea generică la adresa siguranței naționale este atitudinea, exprimată sau nu, a unei puteri sau organizații străine, a unui grup de interese externe sau interne, precum*

——— [120] Antonie Iorgovan, *Tratat de Drept Administrativ* vol.I, Ed. Nemira, București, 1996.

şi a oricăror persoane, asociate ori individual, care prin declaraţiile, acţiunile, măsurile ori poziţiile lor, pun în pericol siguranţa naţională, reprezentată sintetic prin normalitatea raporturilor interne şi externe ale statului, care condiţionează şi garantează dreptul la fiinţă al naţiunii.[121]

În România, întreaga activitate de informaţii este organizată şi coordonată de către Consiliul Suprem de Apărare a Ţării[122], la rândul său, organ central de specialitate al administraţiei de stat, prezidat de Preşedintele României şi controlat de Parlament. Ca principii generale ale activităţii serviciilor de informaţii şi siguranţă naţională din România sunt prevăzute: rezultatele activităţii de informaţii nu pot fi *interpretate sau folosite in scopul restrângerii sau interzicerii dreptului de apărare a unei cauze legitime, de manifestare a unui protest sau dezacord ideologic, politic, religios ori de altă natură, garantate prin Constituţie sau legi; nici o persoană nu poate fi urmărită pentru exprimarea liberă a opiniilor sale politice*; nimeni nu poate viola domiciliul sau proprietăţile unei persoane; nimeni nu poate viola corespondenţa ori comunicaţiile unei persoane; nu pot fi aduse atingeri ale reputaţiei sau onoarei unei persoane.

Aceste principii de legalitate vizează situaţiile în care persoana *„nu săvârşeşte vreuna din faptele ce constituie o ameninţare la adresa siguranţei naţionale.*

Articolele 13[123], 14 şi 15 din Legea Siguranţei Naţionale vizează posibilitatea lucrătorilor ca, în cazurile în care se constată existenţa ameninţărilor, prevăzute în art. 3, să solicite procurorului special abilitat, cu respectarea prevederilor Codului de Procedură Penală, autorizaţia necesară pentru: *„interceptarea comunicărilor, căutarea unor informaţii, documente sau înscrisuri pentru a căror obţinere este necesar accesul*

[121] Aurel Rogojan, *Elemente de drept*-Ed.INI, Bucureşti, 1999.

[122] Atribuţiile Consiliului Suprem de Apărare a Ţării sunt prevăzute in art. 7 din Legea 51/1991

[123] Curte Constituţională a stabilit prin Decizia 341/1997, publicată în Monitorul Oficial nr. 38/1998, că prevederile acestui articol sunt perfect constituţionale şi a respins excepţia de neconstituţionalitate primită.

într-un loc, ridicarea sau repunerea la loc a unui obiect sau document, examinarea lui, extragerea informațiilor pe care acestea le conțin, cât și înregistrarea, copierea sau obținerea de extrase prin orice procedee, instalarea de obiecte, întreținerea și ridicarea acestora din locurile în care au fost dispuse (art. 13, alin. 1). Aducerea la îndeplinire a mandatului conferă *persoanelor împuternicite dreptul de a deține, fără a uza de mijloace de constrângere fizică sau morală, mijloacele adecvate.*

Desfășurarea fără mandat a activităților supuse autorizării, în condițiile art. 13 sau depășirea mandatului acordat, se pedepsește cu închisoare de la 1 la 5 ani. Tot *cu această pedeapsă se sancționează și fapta funcționarului care divulgă, refuză sau împiedică, în orice mod, aducerea la îndeplinire a mandatului eliberat* (art. 20, alin. 2).

Personalul Serviciilor se compune din cadre militare permanente și salariați civili, iar în exercitarea atribuțiilor operative este înzestrat cu exercițiul autorității de stat.

În mod cert în cadrul personalului nu se pot regăsi persoane care au fost găsite vinovate pentu acțiuni îndreptate împotriva drepturilor și libertăților fundamentale ale omului.

RESTRÂNGEREA EXERCIȚIULUI UNOR DREPTURI ȘI LIBERTĂȚI

Declarația Universală a Drepturilor Omului prevede în art. 29, alin. 2 că *în exercitarea drepturilor și libertăților sale, fiecare om nu este supus decât numai îngrădirilor stabilite prin lege, exclusiv în scopul de a asigura cuvenita recunoaștere și respectare a drepturilor și libertăților altora și ca să fie satisfăcute justele cerințe ale moralei, ordinii publice și bunăstării generale, într-o societate democratică.*

În cuprinsul art. 4 din Pactul Internațional cu privire la drepturile civile și politice[124] se prevede că *statul nu poate supune drepturile decât la limitările prevăzute de lege* cu condiția ca acestea să nu fie incompatibile cu celelalte obligații

[124] Ratificat de România prin Decretul nr. 212 din 9 decembrie 1974.

pe care acesta le are potrivit dreptului internațional și ca din ele să nu rezulte o discriminare întemeiată numai pe rasă, culoare, sex, limbă, religie sau origine socială.

Conform prevederilor din Constituția României, exercițiul unor drepturi sau libertăți poate fi restrâns numai printr-o prevedere legală *și numai dacă se impune, după caz, pentru: apărarea securității naționale, a ordinii, a sănătății ori a moralei publice, a drepturilor și libertăților cetățenilor, desfășurarea instrucției penale, prevenirea consecințelor unei calamități naturale, ori ale unui sinistru deosebit de grav.*

Posibilitatea restrângerii prin lege a exercițiului unor drepturi sau a unor libertăți este extrem de vastă, putându-se practic, referi la orice drept sau libertate instituită de legea fundamentală. O clarificare privind această restrângere o găsim în alin. 2 al art. 53 potrivit căruia: *restrângerea trebuie să fie proporțională cu situația care a determinat-o și nu poate atinge existența dreptului sau libertății.*

Legea 51/1991 prevede la art. 13 că lucrătorii (anume desemnați) din domeniul siguranței naționale pot efectua diverse acte, premergătoare urmăririi penale-transformate în mijloace de probă cu respectarea prevederilor Codului de procedură penală, precum: interceptarea comunicațiilor, căutarea unor informații, documente sau înscrisuri pentru a căror obținere este necesar accesul într-un loc, la un obiect sau deschiderea unui obiect; ridicarea și repunerea la loc a unui obiect sau document, examinarea lui, extragerea informațiilor pe care acestea le conțin, cât și înregistrarea, copierea sau obținerea de extraes prin orice procedee; instalarea de obiecte, întreținerea și ridicarea acestora din locurile în care au fost depuse. Temeiul legal stă la baza solicitării procurorului a autorizației necesare efectuării acestor acte.

Analizând rațiunile care stau la baza eliberării mandatului vom constata că acestea se prezintă ca o garanție juridică de respectare a drepturilor și libertăților constituționale. Din primele teze ale art. 13 din Legea 51/1991 rezultă că procurorul va elibera mandatul având în vedere două aspecte fundamentale: existența unei amenințări la adresa siguranței

naționale, din cele prevăzute în art. 3 al Legii 51/1991; solicitarea să se refere la ceea ce legea denumește *„cazuri justificate"*.

Legea protejează *„spațiile închise"*, în care se exercită , firesc, și sunt ocrotite drepturile fundamentale, ca: inviolabilitatea domiciliului și a reședinței, viața intimă, familială și privată(incluzând discuțiile, comunicările, imaginile sau alte activități specifice acestui mediu).

Conform prevederilor Constituției României, exercițiul unor drepturi sau libertăți poate fi restrâns numai printr-o prevedere legală *„și numai dacă se impune, după caz, pentru: apărarea siguranței naționale, a ordinii, a sănătății ori a moralei publice, a drepturilor și libertăților cetățenilor, desfășurarea instrucției penale, prevenirea consecințelor unei calamități naturale, ori ale unui sinistru deosebit de grav"*.

Posibilitatea restrângerii prin lege a exercițiului unor drepturi sau a unor libertăți este extrem de vastă, putându-se practic, referi la orice drept sau libertate instituită de legea fundamentală. O clarificare privind această restrângere o găsim în alin. 2 al art. 49 potrivit căruia: *„restrângerea trebuie să fie proporțională cu situația care a determinat-o și nu poate atinge existența dreptului sau libertății"*.

Legea 51/1991 prevede la art. 13 că lucrătorii (anume desemnați) din domeniul siguranței naționale pot efectua diverse acte, premergătoare urmăririi penale-transformate în mijloace de probă cu respectarea prevederilor Codului de procedură penală, precum: interceptarea comunicațiilor, căutarea unor informații, documente sau înscrisuri pentru a căror obținere este necesar accesul într-un loc, la un obiect sau deschiderea unui obiect; ridicarea și repunerea la loc a unui obiect sau document, examinarea lui, extragerea informațiilor pe care acestea le conțin, cât și înregistrarea, copierea sau obținerea de extrase prin orice procedee; instalarea de obiecte, întreținerea și ridicarea acestora din locurile în care au fost depuse. Temeiul legal stă la baza solicitării procurorului a autorizației necesare efectuării acestor acte.

Solicitarea și realizarea (punerea în lucru a autorizației) se completează cu dispozițiile ordinelor interne ale structurilor de siguranță națională.

Potrivit completărilor și modificărilor aduse Codului de procedură penală[125] înscrisurile, înregistrările audio sau video și fotografiile, constatările tehnico-științifice și expertizele sunt mijloace de probă admise în legislația română.

NATURA JURIDICĂ A MANDATULUI

În interpretarea naturii juridice a mandatului trebuie avute în vedere două aspecte; primul îl reprezintă rațiunile care stau la baza eliberării mandatului, iar al doilea scopul eliberării acestuia.

Analizând rațiunile care stau la baza eliberării mandatului vom constata că acestea se prezintă ca o garanție juridică de respectare a drepturilor și libertăților constituționale. Din primele teze ale art. 13 din Legea 51/1991 rezultă că procurorul va elibera mandatul având în vedere două aspecte fundamentale: existența unei amenințări la adresa siguranței naționale, din cele prevăzute în art. 3 al Legii 51/1991; solicitarea să se refere la ceea ce legea denumește „*cazuri justificate*". Prin noțiunea de amenințare se are în vedere sensul restrâns al noțiunii, adică starea de pericol preinfracțională, care trebuie pusă în evidență prin date și indicii temeinice.

Expresia „*cazuri justificate*" presupune două aspecte care trebuie luate în considerație, in egală măsură, atât de cei care solicită mandatul, cât și de cei care îi eliberează. Primul aspect constă în a evidenția, respectiv, a demonstra necesitatea efectuării activităților prevăzute în mandat: trebuie să se releve că numai prin aceste acte, activități se poate adânci cunoașterea informativă a faptei ori se pot verifica, documenta anumite aspecte referitoare la aceasta. Un alt aspect care rezultă

[125] Legea nr. 141/1996 pentru completarea și modificarea Codului de procedură penală, publicată în monitorul Oficial nr. 289 din 14 noiembrie 1996.

din interpretarea *„cazurilor justificate"* se referă la situațiile în care existența mandatului se impune datorită faptului că activitățile care urmează a fi realizate în baza lui intră în conflict cu dispozițiile constituționale și legale care protejează drepturile și libertățile fundamentale. *Per a contrario,* se apreciază că anumite activități necesare cunoașterii, verificării sau documentării amenințărilor la adresa siguranței naționale pot fi efectuate fără existența mandatului (ex: supravegherea foto-video in spațiile deschise).

În ceea ce privește criteriile stabilirii acelor situații în care activitățile, ce urmează a fi efectuate, pot leza drepturile persoanelor acestea cad în seama exclusivă a factorilor care solicită mandatul și care îl eliberează. Acest demers juridic are la bază prevederile art. 16, alin.1 din Legea 51/1991: *„mijloacele de obținere a informațiilor necesare siguranței naționale nu trebuie să lezeze, în nici un fel, drepturile sau libertățile fundamentale ale cetățenilor, viața particulară, onoarea sau reputația lor, ori să îi supună la îngrădiri ilegale"*, iar pe de altă parte posibilitate instituită de art. 49 din Constituție. *„spațiile inchise"*, în care se exercită, firesc, și sunt ocrotite drepturile fundamentale, ca: inviolabilitatea domiciliului și a reședinței, viața intimă, familială și privată (incluzând discuțiile, comunicările, imaginile sau alte activități specifice acestui mediu). Problema, care se ridică, este dacă se pot desfășura activități de interceptare și înregistrare audio în spații deschise, locuri publice. Răspunsul la întrebare îl dă doctrina: *„...este un atentat la viața intimă a persoanei ascultarea, înregistrarea sau transmiterea, printr-un aparat oarecare, a imaginilor sau vorbelor pronunțate de o persoană, fără consimțământul acesteia"*[126].

Ieșind în public persoana se expune (transmite imaginea sa), dar în ceea ce privește discuțiile trebuie analizat dacă persoana exercită cu bună credință drepturile sale, ceea ce înseamnă că dacă, la adăpostul protecției constituționale a

[126] Constituția României — comentată și adnotată, Ed. Monitorul Oficial, București, 1992, p. 52.

unui drept, comite fapte care contravin legii sau drepturilor celorlalți săvârșește un abuz de drept.

Având în vedere acestea, putem considera că discuțiile care se desfășoară în locuri sau spații circumscrise noțiunii de loc public ar putea fi captate, înregistrate sau transmise fără mandat. Totuși, protecția constituțională a drepturilor nu este condiționată de exercitare lor în anumite locuri.

„*Accesul intr-un loc*" trebuie interpretat în corelație cu definiția locului public dată de art.152, Cod penal; astfel „*locul*" poate fi reprezentat de domiciliu, sediu de firmă, spațiile adiacente acestora etc.

Termenul de mandat, utilizat până acum, este sinonim cu acela de autorizație, utilizat de Codul de Procedură Penală; procurorul, in realizarea atribuțiilor sale, „poate să asiste la efectuarea oricărui act de cercetare penală sau poate să-l efectueze personal" și „conduce și controlează activitatea de cercetare penală" (art.218, Cod de Procedură Penală). Luând în considerație și prevederile art.13 al Legii 14/1992 și faptul că aceste activități au caracter secret de stat și extrajudiciar procurorul nu poate îndeplini cu privire la ele nici una din atribuțiile prevăzute de art. 218–220 Cod de procedură Penală; astfel „autorizația" surprinde mai bine conținutul și structura actelor care trebuie efectuate, procurorul „autorizând" organele de siguranță națională la desfășurarea unor activități pe care el nu le efectuează.

Eliberarea mandatului are, din punct de vedere juridic, următoarele consecințe: restrânge exercițiul unor drepturi și libertăți fundamentale; acordă protecție juridică persoanelor abilitate să îl execute; rezultatele obținute pot fi în valorificate în documente juridice cu valoare probatorie.

RESTRÂNGEREA UNOR DREPTURI ÎN PRACTICA SERVICIILOR SECRETE STRĂINE

În Marea Britanie, Legea privind secretele de stat a împiedicat permanent publicarea unor informații despre structurile

informative. În orice caz, în Regat, și nu numai aici, acestea se bucură de un respect deosebit.

Principalele surse de informații secrete sunt ascultarea și interceptarea comunicațiilor, supravegherea, precum și agenții. Ascultarea înseamnă interceptarea secretă a convorbirilor obiectivelor. Este posibilă și interceptarea clandestină atât a comunicațiilor poștale, cât și a celor telefonice.

Interceptarea comunicațiilor poștale și telefonice se poate efectua numai în baza emiterii, în mod expres, a unui mandat special, în conformitate cu Legea nr. 56 /1985. În plus, în cazul în care se apreciază că operațiunile de ascultare reprezintă un amestec ilegal în proprietatea unei persoane, este necesară, în conformitate cu Legea Serviciului de Securitate, obținerea unui *„mandat cu drept de intrare într-o proprietate privată"*.

Mandatele eliberate de Secretarul de Stat[127] vor trebui să aibă la bază informații care atestă că acestea sunt necesare: *„a) în interesul securității naționale; b) în scopul prevenirii sau descoperirii unor infracțiuni; c) în scopul de a apăra bunăstarea economică a Regatului Unit"*, (art. 2(2), Legea 56/ 1985).

În considerarea necesității mandatului se va analiza foarte serios dacă informația care este considerată necesară ar putea fi *„în mod rezonabil, obținută pe alte căi"*. Cererea de mandat trebuie să cuprindă natura amenințării, să motiveze necesitatea propunerii de interceptare, și să confirme că obiectivul operațiunii se încadrează în atribuțiile Serviciului.

Supravegherea reprezintă *„observarea vizuală"* a vectorilor, în scopul obținerii de informații referitoare, de exemplu, la deplasările pe care le fac, precum și la identitatea celor cu care obiectivele se află în legătură.

Interceptarea ilegală se face prin recrutarea unor persoane din serviciile care asigură comunicațiile.

---

[127] Art. 2. (1) *...Secretarul de Stat poate emite un mandat prin care solicită persoanei căreia îi este adresat să intecepteze, în cursul transmiterii prin poștă sau prin mijloace ale sitemului de telecomunicații, comunicările care vor fi descrise în mandat...* (Legea 56/1985).

Supravegherea juridică se realizează, conform Legii privind interceptarea comunicațiilor de către un Tribunal pentru analizarea reclamațiilor la adresa Serviciului, înaintate de public[128]. Legea stipulează că orice persoană poate adresa reclamații Tribunalului „*dacă consideră că Serviciul a adus atingere propriei sale persoane sau dreptului său de proprietate*". Dacă reclamația este întemeiată, Tribunalul are autoritatea să dispună încheierea investigațiilor și distrugerea înregistrărilor, precum și plata unor despăgubiri.

În Franța, Legea interceptărilor[129] nr. 91–646 a fost promulgată la 10 iulie 1991, astfel aria interceptărilor fiind limitată scopurilor privind securitatea națională.

Art. 1 (2) din Lege prevede că se poate aduce atingere secretului corespondenței dacă este o necesitate a interesului public. Art. 4 precizează că autorizația este acordată prin decizie „*scrisă și motivată a Primului Ministru sau a uneia dintre cele două persoane special delegate de acesta*". Această autorizație este dată pe propunerea scrisă și motivată a ministrului apărării naționale sau a ministrului de interne. Activitățile care au ca obiect interceptarea corespondenței sunt supuse controlului Comisiei Naționale de Control a Interceptărilor de Securitate, autoritate administrativă independentă.

Practica demonstrează că acolo unde D.S.T.-ul nu poate pătrunde legal cu mijloacele de interceptare, se poate recurge la diverse formațiuni private, formate din specialiști în rezervă ai serviciilor secrete.

Centrul de ascultări radio și interceptări telefonice funcționează sub acoperirea Grupului Interdepartamental de Control și este conceput pentru a intercepta orice fel de comunicații.

---

[128] Art.7 (2): *Orice persoană care este de părere că au fost interceptate comunicațiile transmise prin sistemul de telecomunicații public sau poștă poate apela la Tribunal pentru a efectua o investigație în acest sens.*

[129] Titlul II, art.3 *Pot fi autorizate, cu titlu excepțional, interceptările corespondențelor transmise pe calea telecomunicațiilor, ce au ca obiect cercetarea informațiilor care interesează securitatea națională, apărarea elementelor esențiale ale potențialului științific și economic al Franței, sau prevenirea terorismului, a criminalității și a delincvenței organizate.*

Pentru aprobarea unei interceptări există o singură condiție de fond, aceea ca fapta ce se cere stabilită să fie sancționată penal cu cel puțin doi ani de închisoare.

Interceptările telefonice pot fi efectuate pe durata a patru luni,[130] față de două în Germania sau trei, în Anglia. Majoritatea centralelor telefonice din Franța este conectată, printr-un hard și soft deosebit, la Centrul de ascultare și interceptări telefonice.

În Germania, o lege specială, cunoscută sub denumirea de *„G–10"* [131], reglementează condițiile în care se poate uza de interceptări[132] și anume: existența unor infracțiuni sigure și grave, precum înaltă trădare, constituirea unor organizații teroriste[133]; imposibilitatea ca activitățile secrete ori periculoase să poată fi descoperite pe altă cale [134].

Autorizarea interceptării este dată de ministrul de Interne. Înainte de apicarea autorizării, Comisia *„G–10"*, (organism independent compusă dintr-un președinte (judecător) și doi membri, hotărăște cu privire la oportunitatea măsurilor de limitare a drepturilor. În situație de urgență, autorizarea se pune în aplicare fără hotărârea comisiei, aceasta fiind infor-

[130] Art. 6 prevede ca durată a autorizației termenul de patru luni.

[131] Legea privind limitarea secretului corespondenței, trimiterilor poștale și a convorbirilor telefonice, publicată în Monitorul Oficial nr. 57 / 15 august 1968.

[132] Art. 1 §1. (1) *...organele federale și locale de securitate, serviciile de securitate ale armatei federale, precum și serviciile de informații externe au dreptul să aibă accs la expediții și emisiuni ce intră sub incidența secretului corespondenței și al telecomunicațiilor, precum și să citească ccorespondența telegrafică și să intercepteze și să înregistreze pe suporți magnetici traficul de telecomunicații.*

[133] *§ 2. (1) Pot fi dispuse îngrădiri (...) dacă există dovezi clare care să susțină bănuiala că o persoană plănuiește, săvârșește sau a săvârșit:*
1) infracțiuni contra păcii sau de înaltă trădare;
2) infracțiuni de periclitare a statului de drept democratic;
3) infracțiuni de trădare națională și de periclitare a securității externe;

[134] § 2. (3) O astfel de dispoziție este permisă numai dacă cercetarea stărilor de fapt nu este altfel posibilă sau esențial îngreunată.

mată ulterior. Dacă nu este de acord măsura luată trebuie să înceteze.

Semestrial o comisie parlamentară, formată din cinci deputați, se informează asupra situațiilor care au făcut obiectul Legii *„G–10"*.

Astfel, Comisia *„G–10"* și Forul *„G–10"* apreciază aprobarea și necesitatea luării măsurilor de limitare a secretului corespondenței.

După încetarea măsurilor de repective, dacă nu există pericolul prejudicierii scopului urmărit, acestea pot fi aduse la cunoștința persoanelor vizate. Dacă cerința nu poate fi îndeplinită în termen de 5 ani, obligația încunoștiințării încetează.

Fiecare persoană are dreptul legal de a se opune, pe cale juridică, măsurilor luate de B.F.V., adresându-se în acest scop, unui tribunal special independent, pentru verificarea legalității acestora. Această posibilitate este vizată de Legea *„G–10"*.

Recent, în „Tageszeitung" (nr. din 23.03.2004) a apărut un articol referitor la faptul că *„Serviciul Federal de Informații interceptează zilnic 100.000 de convorbiri telefonice, dintre care 75.000 în Germania, dar numai trei sunt supravegheate în continuare"* — a declarat Volker Homuth, președintele Oficiului de Land pentru Apărarea Constituției din Saxonia Inferioară. *„Serviciile secrete pot sparge orice formă de codificare"* — a declarat însărcinatul pentru protecția datelor din landul Brandenburg.

În Italia, prin Decretul Lege nr. 345, din 29 octombrie 1997, se aduc modificări Codului Penal — art. 616- 619 și 623 bis și de Procedură Penală. Aceste articole incriminează orice cunoaștere, întrerupere, împiedicare sau interceptare, în afara cazurilor prevăzute de lege. Prin aceste modificări art. 254 Codul de Procedură Penală dispune: *„În oficiile poștale sau telegrafice este permisă procedarea la sechestrarea de scrisori, colete, pachete, valori, telegrame și alte obiecte de corespondență pe care autoritatea judiciară are motiv să le considere ca expediate de inculpat sau adresate acestuia"*.

Autorizația este solicitată judecătorului de către procuror, putând fi acordată numai printr-o decizie motivată, *atunci*

când există indicii serioase ale unei infracțiuni și interceptarea este absolut indispensabilă (art. 267, alin.1). *În cazuri de urgență, când există un motiv întemeiat, procurorul dispune interceptarea cu o decizie motivată, care trebuie imediat comunicată, dar nu mai târziu de 24 de ore, judecătorului* (art. 267, alin.2).

În sistemul juridic italian este prevăzută *„interceptarea preventivă"*; astfel ministrul de interne, responsabilii la nivel central ai serviciilor centrale și interprovinciale sau procurorul Republicii pot autoriza printr-o decizie interceptarea comunicațiilor telefonice și a altor forme de comunicare, când sunt necesare pentru activitatea de prevenire și informare. De subliniat este că interceptările preventive *„sunt lipsite de orice valoare procesuală"*.

În SUA, principalul serviciu de spionaj, CIA îndeplinește orice activitate, dacă se consideră că interesele naționale o cer. În privința surselor tehnice, pentru realizarea de instalații care impun intervenții pe rețeaua telefonică, toate stațiile CIA au sarcini de recrutare de agenți de sprijin în rândul personalului companiilor telefonice locale.

Interceptarea convorbirilor purtate în locuri de interes situate în apropierea reprezentanțelor diplomatice, comerciale sau militare americane se realizează și prin mijloace care utilizează fascicole de laser sau radiații infraroșii, pentru preluarea vibrațiilor ferestrelor. Interceptarea corespondenței se realizează prin agenturi de legătură cu serviciile locale de securitate sau prin operațiuni unilaterale.

Agenția pentru Securitate Națională (NSA) componentă integrantă a Ministerului Apărării are ca obiectiv principal acela de a supraveghea orice semnale electronice, scop în care ascultă toate convorbirile telefonice.

În subordinea sa se află sistemele americane globale de interceptare a comunicațiilor altor națiuni[135].

[135] *Echelon* este sistemul american de supraveghere globală și poate capta până la două milioane de convorbiri pe minut, misiunea sa fiind aceea de a urmări guvernele, organizațiile și firmele.

Toate comunicațiile de pe glob pot fi captate de sateliți sincronizați, care retransmit semnalele printr-un cablu de 500.000 fire la Centrul de Telecomunicații.

În practica FBI (Biroul Federal de Investigații, care face parte din Ministerul Justiției) obținerea de informații prin interceptări se realizează numai cu aprobarea Procurorului General. Solicitarea autorizației se face de către judecători și procurori special desemnați. Raportul judecătorului cuprinde: motivația, mijlocul tehnic utilizat, durata și identitatea oficialităților guvernamentale, care cer supravegherea.

Patriot Act (recent adoptat) accentează importanța serviciilor de securitate Națională a SUA, permițând acestora desfășurarea oricăror activități de natură restrictivă în domeniul drepturilor și libertăților cetățenești, mai ales că din partea societății civile există o deosebită înțelegere a unor astfel de măsuri.

De interes pentru tema abordată sunt și praticile serviciilor secrete israeliene. Mossad-ul este un serviciu secret care aflându-se în permanent război acționează de fiecare dată în împrejurări excepționale, neformalizându-se în ce privește drepturile și libertățile fundamentale.

În Israel, ca și în străinătate, sunt practicate pătrunderile secrete în reședințe, birouri, domicilii, autoturisme, obținerea de fotocopii și documente. Pentru aceasta cooperează larg cu firmele ce produc echipamente de securitate.

Ofițerii nu sunt specializați doar în efracții, ci se pricep la elaborarea complexului de măsuri combinative prin care să faciliteze accesul. La încheierea studiilor, aceștia dau probe practice complexe în acest sens.

Departamentul Tehnic de Interceptare (SHIKLUT) realizează interceptarea comunicațiilor sau a convorbirilor de interes, în orice loc din lume este necesar, după care înregistrările ce se impun a fi traduse ori decodificate sunt transmise pentru procesare la centrala Tel Aviv.

Unitatea 8200 specializată în interceptările din țările arabe are acces total la ce se transmite prin cablul submediteranean, care este conectat la Palermo cu rețeaua de comunicații prin satelit.

Cadrul legal al interceptărilor îl constituie Legea privind Interceptările din 1979. Potrivit acestei legi ministrul apărării va prezenta, in fiecare an, un raport în fața Comisiei Comune a Kneset-ului pentru probleme constituționale, de drept și justiție și Comisiei pentru Securitate și Afaceri Externe cu privire la numărul de autorizații emise în conformitate cu prevederile acestei legi.

În anul 2001 Ariel Sharon, premierul israelian, a cerut Kneset-ului adoptarea unei legi care să autorizeze serviciile de securitate să utilizeze tortura împotriva deținuților arabi, in condițiile in care sunt interogați zilnic mii de palestinieni suspecți de terorism.

CONCLUZIE

Concluzia de ansamblu ce poate fi desprinsă din studiul evoluției activității postrevoluționare a structurilor de siguranță națională pentru realizarea atribuțiilor conferite prin lege pe coordonatele standardelor internaționale privind drepturile omului și libertățile fundamentale este că aceasta a înregistrat un curs ascendent, odată cu tendințele de stabilizare a vieții politice, economice și sociale. Operatorul de informații a devenit conștient de necesitatea respectării drepturilor omului, ca o coordonată a tuturor activităților pe care le întreprinde. De asemenea, pregătirea ofițerilor s-a diversificat, personalul compunându-se din persoane cu studii superioare, majoritatea cu studii postuniversitare de aprofundare.

Diversificarea metodelor infractionale ale persoanelor care atentează la siguranța națională impune acțiuni noi, care trebuie să se afle în continuare pe linia apărării drepturilor cetățenilor.

Din cele prezentate în structura lucrării reiese că activitatea de înfăptuire a siguranței naționale de către organele române de specialitate se subordonează clar principiilor de drept și regulilor constituționale; acțiunile unor ofițeri, care la adăpostul *interesului de stat*, își rezolvă diverse interese sunt grav sancționate.

Structurile române se situează, în problematica restrângerii exercițiului unor drepturi și libertăți fundamentale, în limitele legale, deosebindu-se de practica structurilor străine, care își permit acțiuni mult mai largi, uneori în baza cadrului legal mai permisiv, dar de cele mai multe ori în afara cadrului legal, justificând toate acestea prin majore interese de stat. În ceea ce privește controlul indirect, în cazul acestor structuri străine, prin intermediul mass-media, se remarcă respectul deosebit acordat acestora, publicarea unor materiale sau acțiuni elogiind întotdeauna profesionalismul operatorilor și acceptând că această activitate, chiar atunci când se restrâng drepturi și libertăți fundamentale, este de importanță deosebită pentru existența statului de drept.

PARTICULARITĂȚI ALE ACTIVITĂȚII ȘI FACTORILOR DE RISC CE POT AFECTA EXECUTAREA PAZEI CU EFECTIVE DE JANDARMI

Claudiu Lepădatu

Prin structura și atribuțiile conferite de prevederile Legii nr. 116 din 18.06.1998, Jandarmeria Română asigură paza și apărarea unor obiective, a bunurilor și valorilor de importanță deosebită, menținerea și restabilirea ordinii publice, prevenirea și combaterea infracțiunilor și a altor încălcări ale normelor legale în vigoare, precum și participarea alături de celelalte structuri abilitate la prevenirea și neutralizarea actelor teroriste și de diversiune pe teritoriul României.

În afara obiectivelor pozitive spre care se aspiră, ca urmare a transformărilor la care este supus Ministerul Administrației și Internelor și structurile sale inclusiv Jandarmeria Română procesul generează o complexitate de vulnerabilități și factori de risc care se impun a fi identificați și gestionați concomitent cu determinarea cauzelor care îi creează și care necesită luarea unor contramăsuri de înlăturare a efectelor negative apărute, unele în mod obiectiv, dar altele determinate și de condiții subiective.

Multitudinea misiunilor desfășurate de către unitățile și marile unități din compunerea Jandarmeriei Române a impus crearea unei palete largi și diversificate de măsuri pentru protecția efectivelor și misiunile acestora.

CADRUL JURIDIC AL DESFĂȘURĂRII ACTIVITĂȚILOR SPECIFICE

În conformitate cu art.6 din Legea nr. 51/1991, organele de stat cu atribuții în domeniul siguranței naționale sunt: Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Protecție și Pază, precum și Ministerul Apărării

Naţionale, Ministerul Administraţiei şi Internelor şi Ministerul Justiţiei prin structuri interne specializate. De asemenea, la art. 9 din cadrul aceleiaşi legi se stipulează faptul că *„Ministerul Apărării Naţionale, Ministerul Administraţiei şi Internelor şi Ministerul Justiţiei îşi organizează structuri de informaţii cu atribuţii specifice domeniilor, lor de activitate"*.

În acest context conform art.1 din Regulamentul privind organizarea şi funcţionarea unităţii, Direcţia Generală de Informaţii şi Protecţie Internă este unitatea componentă a aparatului central al Ministerului Administraţiei şi Internelor, specializată în obţinerea, verificarea, valorificarea şi stocarea de informaţii şi date necesare realizării atribuţiilor ce revin ministerului conform legii şi este subordonată nemijlocit ministrului.

Activitatea Direcţiei Generale de Informaţii şi Protecţie Internă este pusă sub controlul Parlamentului şi se desfăşoară în conformitate cu prevederile Constituţiei României, a legilor, tratatelor şi convenţiilor internaţionale, a hotărârilor Consiliului Suprem de Apărare a Ţării şi ale Guvernului, ordinelor şi instrucţiunilor ministrului administraţiei şi internelor, astfel încât să nu lezeze drepturile şi libertăţile omului, să asigure deplina neutralitate faţă de orice ingerinţă sau interes, să promoveze obiectivitatea, realitatea, legalitatea şi deplina responsabilitate a acţiunilor sale.

Activitatea ofiţerilor de protecţie internă se desfăşoară pe principiul muncii în obiectiv şi se realizează prin metode şi mijloace specifice, prin culegere de date şi informaţii de interes operativ necesare pentru asigurarea protecţiei unităţilor din responsabilitate, cu respectarea strictă a prevederilor legale care constituie fundamentul activităţii Direcţiei Generale de Informaţii şi Protecţie Internă.

Astfel, activitatea specifică a unităţii este reglementată prin Legea nr.40/1990 privind organizarea şi funcţionarea Ministerului Administraţiei şi Internelor, Legea nr.51/1991 privind siguranţa naţională a României, Ordinul ministrului administraţiei şi internelor nr.II/0010.011 din 01.03.2003 pentru aprobarea Regulamentului privind organizarea şi funcţionarea Direcţiei Generale de Informaţii şi Protecţie Internă,

Din cele 1181 obiective cărora Jandarmeria Română le asigură în prezent paza, cel puțin 795 sunt expuse riscului de a fi ținta unor acte sau acțiuni cu caracter terorist, având în vedere importanța și destinația lor (129 obiective sunt de importanță deosebită pentru siguranța națională, 256 pentru activitatea statului, 164 sunt obiective diplomatice și 266 aparțin Ministerului Administrației și Internelor).

Menționăm totodată că Jandarmeria Română participă din anul 2002 cu un detașament de jandarmi la misiuni de menținere a păcii sub egida ONU, în Kosovo.

Din această perspectivă și în contextul evoluției situației operative în zona Golfului Persic s-a impus redimensionarea conceptului de protecție informativă a personalului, misiunilor și patrimoniului Jandarmeriei Române, împotriva oricăror acțiuni de natură extremist — teroristă, cu următoarele obiective:

– desfășurarea activităților specifice de culegere de date și informații privind prevenirea, descoperirea și documentarea acțiunilor prin care se urmărește pregătirea unor acte teroriste, ce ar putea viza personalul, obiectivele proprii, cât și cele date în competență, precum și misiunile încredințate efectivelor de jandarmi;

– identificarea și prevenirea unor posibili factori de risc și amenințări pe linia pazei și protecției unităților proprii, cât și a celor de importanță deosebită date în pază structurilor specializate de jandarmi, în special a celor vulnerabile la terorism;

– prevenirea și contracararea oricăror factori de risc și amenințări îndreptate împotriva efectivelor de jandarmi care participă la misiuni internaționale de menținere a păcii;

– analiza periodică a datelor și informațiilor obținute privind evoluția situației operative de pe spațiul Jandarmeriei Române, în concordanță cu evoluția situației la nivel național și internațional, pentru a putea anticipa riscurile pentru siguranța instituției pe profilul combaterii terorismului.

Posibilii factori de risc și amenințări cu care se pot confrunta marile unități și unitățile de jandarmi:

– producerea unor acte teroriste cu sau fără luarea de ostateci, la obiectivele din competență sau la alte obiective de importanță deosebită din zonele de responsabilitate;

– producerea unor atacuri armate, în scop de jaf, asupra unor instituții financiar-bancare sau asupra unor transporturi importante de valori;

– atacuri îndreptate asupra unor transporturi speciale, respectiv de armament, muniție, materiale explozive sau radiologice, ori a altor materiale și substanțe periculoase;

– acțiuni asupra conductelor magistrale de transport produse petroliere, în scopul sustragerii de astfel de produse sau de poluare a mediului;

– producerea de accidente chimice sau radiologice la obiectivele a căror pază este asigurată de efective de jandarmi, ce pot pune în pericol grav populația;

– culegerea de date și informații cu caracter secret de stat și de serviciu din obiectivele asigurate cu pază de jandarmi, în scopul inițierii unor astfel de acțiuni;

– acțiuni în forță îndreptate împotriva elementelor de dispozitiv la obiective izolate, date în competență, în scopul procurării de armament și muniție.

În conformitate cu atribuțiile și competențele stabilite de normele legale care reglementează activitatea de protecție, se obțin date și informații pe baza cărora sunt identificate elemente și factori de risc care caracterizează și influențează în mare parte evoluția situației operative în obiectivele date în răspundere, permițând totodată stabilirea celor mai eficiente căi de intervenție preventivă.

VULNERABILITĂȚI ȘI FACTORI DE RISC

La nivelul unităților din structura Comandamentului Național al Jandarmeriei situația informativ–operativă poate fi caracterizată ca fiind dinamică și complexă, iar din analiza acesteia rezultă câteva aspecte esențiale.

1. Vulnerabilități în dispozitivele de pază constituite cu efective de jandarmi la obiectivele de importanță deosebită.

Din analiza datelor privind sistemele de pază din competența unităților de jandarmi, rezultă unele vulnerabilități ce pot fi exploatate de persoane interesate în inițierea unor acțiuni de natură extremist — teroristă, sens în care exemplificăm:

– menținerea în dispozitivul de pază a militarilor în termen, care nu au o pregătire specifică și capacități necesare realizării unei intervenții optime în cazul unui eventual atac de natură extremist–teroristă, iar trăsăturile psiho-afective și comportamentale ale acestei categorii de personal pot genera producerea unor evenimente deosebite. Mai mult, în unele cazuri, datorită insuficienței efectivelor, s-a procedat la reducerea posturilor de santinelă.

– deficitul de personal specializat, respectiv jandarmi angajați pe bază de contract, destinat pazei, acumulat prin blocarea funcțiilor, urmare a transferului la Poliția de Frontieră în 2001, demisiile sau desfacerea contractului de muncă din motive disciplinare, precum și insuficiența celui existent la obiectivele de importanță deosebită constituie în egală măsură, vulnerabilități în sistemul de pază.

– la unele obiective, eficiența dispozitivului de pază este scăzută și din cauza lipsei instalației de iluminare pe timp de noapte, a gardului împrejmuitor sau în unele cazuri, lipsei împrejmuirii pentru pistele de aterizare — decolare.

– posibilitatea pătrunderii în obiectivele date în competență a unor persoane interesate, având asupra lor armament, muniție, substanțe explozive sau alte materiale periculoase.

De asemenea, datorită faptului că punctele de control — acces de la sediile obiectivelor date în competență și asigurate permanent cu subofițeri jandarmi nu sunt dotate cu mijloace tehnice specifice de control antiterorist, astfel încât persoane interesate în inițierea unor acțiuni de natură extremist — teroristă pot intra ilegal în obiective cu astfel de materiale asupra lor.

2. Menținerea unor disfuncționalități privind planificarea și organizarea efectivelor participante la misiuni specifice de pază și supraveghere, atrage suprasolicitarea personalului destinat la astfel de activități, precum și diminuarea capacității de acțiune și intervenție la celelalte misiuni de la care

au fost detașate efective pentru noile misiuni preluate în competență.

Exemplificăm situația creată la nivelul Comandamentului de Jandarmi Județean Buzău privind asigurarea efectivelor destinate pazei conductelor petroliere care tranzitează județul Buzău (tronson de aproximativ 30 km între locațiile Săbăreni și Gălbinari), preluate de la 01.01.2002 de la Batalionul Special de Jandarmi Ploiești, dar cu efective detașate de la Comandamentul de Jandarmi Buzău.

Prin detașare au fost diminuate efectivele destinate celorlalte activități specifice, respectiv efectivele Detașamentului Mobil, fiind reduse unele funcții. În consecință nu se mai asigură condiții normale de activitate atât pentru paza și supravegherea conductelor cât și pentru celelalte activități.

Semnificativă este și situația creată la Comandamentul de Jandarmi Județean Brașov, unde potrivit Ordinului M.A.I. nr.S/233 din 01.04.2002 privind paza și apărarea obiectivelor date în competență trupelor de jandarmi, art.194 prevede că subofițerii vor fi organizați în serviciu câte 12 ore/zi, fără a depăși 180 ore/lună, iar la anexa nr.3 din același ordin se prevede ca un post de pază și control — acces să fie încadrat cu 5 subofițeri.

Datorită deficitului de personal, posturile sunt asigurate cu câte 4 subofițeri, astfel încât asigurarea serviciilor în paralel cu respectarea concediilor de odihnă, cu acordarea celor medicale sau de studii se face prin forțări, cadrele ajungând să depășească frecvent peste 250 ore/lună, aspect ce duce la diminuarea calității serviciilor prestate de aceștia.

Situațiile semnalate nu sunt izolate, cazuri similare privind disfuncționalități în planificarea subofițerilor, jandarmilor angajați pe bază de contract și militarilor în termen se regăsesc la foarte multe din marile unități și unități de jandarmi, sens în care exemplificăm Comandamentele de Jandarmi Județene Timiș, Călărași, Galați, Dolj și Buzău.

3. Interesul manifestat de cetățeni străini sau români în prospectarea obiectivelor de importanță deosebită la care se execută misiuni specifice de pază cu efective ale Jandarmeriei Române, cât și la sediile marilor unități și unităților de jandarmi.

Astfel, la data de 12.02.2003 a fost semnalată prezența autoturismului Dacia, având numărul de înmatriculare CT-05-HJU, în care se aflau două persoane ce filmau Aeroportul „Mihail Kogălniceanu" — Constanța. Verificările efectuate au scos în evidență că la acea dată, pe aeroport nu staționau trupe americane și nu funcționa actualul dispozitiv de pază și supraveghere. Din investigațiile efectuate a rezultat că numărul menționat era fals, acesta fiind atribuit unui alt autoturism ce aparținea unui cetățean din municipiul Constanța.

De asemenea, a fost semnalată prezența repetată a unor autoturisme ce aparțin corpului diplomatic în zona cazărmii din municipiul Orăștie.

4. Se menține intenția persoanelor din lumea interlopă, de a cultiva relații cu cadre de jandarmi, în special a celor care execută misiuni de pază și apărare a instituțiilor financiar — bancare și a transporturilor de valori.

În acest sens, menționăm situația de la Comandamentul de Jandarmi Județean Hunedoara unde numiții Hotaria Petru și Donc Marius, persoane din lumea interlopă, ambii din comuna Jilia, județul Hunedoara, au fost semnalați cu intenții de a atrage la activități ilicite a unui subofițer din cadrul marii unități care își desfășoară activitatea în cadrul grupei de transport valori monetare a „Banc Post". Din verificări a rezultat că, pe timpul desfășurării misiunilor specifice, subofițerul încălca consemnul, oprind autospeciala de transport pentru a se întâlni cu sus-numiții, la popasurile aflate în traseu.

5. Interesul manifestat de grupări infracționale în studierea și prospectarea dispozitivelor de pază și intervenție la conductele magistrale de transport produse petroliere.

Din analiza datelor și informațiilor obținute în ultima perioadă de timp, a rezultat tendința de creștere a interesului manifestat de elemente infractoare de a își crea și permanentiza relații în rândul efectivelor de jandarmi, desemnate să execute misiuni specifice în paza conductelor din zona de competență, în scopul cunoașterii programului de livrare și transport a produselor petroliere, cât și obținerii „protecției" în sustragerile de combustibil, prin atragerea acestora la astfel de activități ilicite.

Semnificativă este situația creată la Batalionul Special de Pază și Intervenție Ilfov, unde jandarmi angajați pe bază de contract destinați misiunilor de pază a conductelor de transport produse petroliere aparținând S.C. PETROTRANS S.A., au fost contactați de lideri ai unor grupări infractoare, semnalate cu preocupări în sustragerea de produse petroliere, în scopul acordării de „protecție" pe timpul desfășurării activităților infracționale.

Astfel, prin măsuri informativ–operative complexe și în cooperare cu Parchetul Național Anticorupție, au fost identificați jandarmi angajați pe bază de contract care în schimbul unor importante sume de bani au semnalat elementelor infractoare zilele și orele când se pompa carburant, asigurându-le totodată protecția pe timpul cât aceștia sustrăgeau produse petroliere.

În prezent activitatea infracțională a jandarmilor angajați pe bază de contract, cât și a celorlalte elemente infractoare este cercetată de Parchetul Național Anticorupție.

O situație aparte s-a constatat la nivelul Comandamentului de Jandarmi Județean Călărași, unde numiții Margovici Puiu Cătălin, angajat la Stația de pompare „Dragoș Vodă" și Breazu Ion Daniel, fără ocupație, din aceeași comună, lideri ai unei grupări infracționale, cu participarea și sub protecția agenților principali de poliție Dumitru Cornel și Cătălin ssorin Romeo, ambii de la Postul de Poliție Dragoș Vodă, au încercat să atragă la colaborare jandarmi angajați pe bază de contract, promițându-le sume de bani cuprinse între 7 și 10 milioane lei, pentru fiecare sustragere „protejată", în scopul neobservării activităților infracționale ale acestora.

Cazuri similare au mai fost semnalate la Comandamentele de Jandarmi Județene Ilfov, Constanța și Dâmbovița, astfel:

– jandarmul angajat pe bază de contract Lefter Ștefan din cadrul Comandamentului de Jandarmi Județean Constanța, a fost contactat de o persoană necunoscută, care s-a recomandat a fi agent de pază la o societate de profil din București și care i-a propus, contra sumei de 1.000 USD / cisternă, să-i asigure protecție pe timpul sustragerii de produse petroliere;

– jandarmii angajați pe bază de contract Andrei Nicușor și Diaconu Ionuț, ambii din cadrul Comandamentului de Jandarmi Județean Ialomița, au fost contactați în același scop de elemente din lumea interlopă, suspecți privind implicarea în activități ilicite, îndeosebi în sustragerea și comercializarea de produse petroliere.

Totodată, au fost identificate persoane, foști agenți de pază, care au manifestat interes în cunoașterea programului de transport produse petroliere.

6. Deficiențe privind dotarea și asigurarea cu mijloace de transmisiuni și de legătură. Calitatea misiunilor de pază, precum și capacitatea de intervenție sunt diminuate de gradul de asigurare de către beneficiarii de pază a mijloacelor de transport corespunzătoare, cât și a mijloacelor de transmisiuni performante sau a sistemului de legătură, atât în cazul pazei instituțiilor bancare, a transportului de valori, cât și a pazei conductelor magistrale de transport produse petroliere.

Menționăm că în aceste situații, conceptul de pază, supraveghere și intervenție se realizează printr-un sistem integrat de posturi fixe și mobile, combinate cu elemente tehnice și electronice, susținute de mijloace de transport, de sisteme de supraveghere și legături radio.

Astfel, în cazul producerii unui eveniment, grupele de intervenție să poată interveni în timp real, întărind acțiunea elementelor de dispozitiv.

În cazul misiunilor de pază și intervenție la instituțiile financiar-bancare, sunt frecvente situațiile în care mijloacele de transport sunt neadecvate și nu corespund conform normelor în vigoare, astfel încât pentru prevenirea producerii unor evenimente deosebite, a fost luată măsura ca pe aceste autovehicule, în cazul unor transporturi de valori, să fie repartizate două cadre de jandarmi.

De asemenea, sunt zone unde stațiile de emisie recepție, fiind necorespunzătoare din punct de vedere tehnic, nu asigură legătura cu transportul, astfel încât unele porțiuni de traseu în teritoriu nu sunt acoperite, legătura realizându-se prin telefonia mobilă.

Vulnerabilitățile sunt create și de lipsa mijloacelor auto pentru personalul destinat misiunilor de pază și intervenție la conductele magistrale de transport produse petroliere, unde zona de competență în acest caz, acoperă distanțe mari, uneori de 15–20 km.

În multe situații, acestea sunt asigurate de către elemente de dispozitiv constituite în patrule pedestre, prilej cu care sunt parcurse trasee de multe ori vulnerabile (zone împădurite, subtraversează linii de cale ferată, traversează pe anumite porțiuni cursuri de apă, diguri pentru irigat etc.), chiar personalul putând fi ținta unor atacuri, în condițiile în care deține armament și muniție.

BIBLIOGRAFIE

Legea nr. 40/1990 — privind organizarea și funcționarea Ministerului Administrației și Internelor; Legea nr. 51/1191 — privind Siguranța Națională a României;

Ordinul M.A.I. nr.II/0010011 din 01.03.2003 — pentru aprobarea Regulamentului privind organizarea și funcționarea D.G.I.P.I.;

Instrucțiunile M.A.I. nr.II/008073 din 04.10.1999 — privind organizarea activității informativ operative a D.G.I.P.I.; Cazuistica de profil.

VI. NOI ABORDĂRI, TENDINȚE ȘI REFLEXII — ÎNTRE TRADIȚIE ȘI MODERNITATE

O ANALIZĂ A TENDINȚELOR ÎN MANAGEMENTUL DE SECURITATE NAȚIONALĂ

Silviu Nate

CÂND TE CONFRUNȚI CU NOI ÎNTREBĂRI, VEI REPLICA CU RĂSPUNSURI TRADIȚIONALE? SAU CU UNELE NOI?

Pornind de la mesajul pentru anul 2004 al companiei de consultanță, tehnologie și outsourcing: *accenture*, nu putem ignora faptul că au venit timpuri când: „cea mai bună lovitură de succes nu este și cea mai evidentă"[136]. Pentru a vedea cum ne putem proteja puterea de inovație în obținerea de performantă maximă, este de cele mai multe ori nevoie de o abordare interdisciplinară. Un accent important îl are atenția concentrată cu precădere pe domeniile și mediile care dezvoltă cele mai eficiente practici la nivelul de concepere și elaborare a strategiilor competiționale și tactice, a planificării, alocării resurselor, implementării, monitorizării, evaluării proceselor organizaționale și de proiect.

Nu ar fi pentru prima data în istorie când metodologia de abordare, tratare și rezolvare a problemelor din domeniul securității naționale este extrasă din, și corelată la practicile și tendințele din mediul economic competițional, în special din cel al business-ului de corporație. Acestea permit dezvoltarea și aplicarea unor sisteme de analiză specifice și procedee

[136] *Accenture*, în „The Economist", p. 10 — 11, 6 martie, 2004.

de lucru personale, cum ar fi: *benchmarking-ul, intelligence-ul competitiv, managementul strategic* și *al riscului, reengineering-ul, etc.* — termeni a căror aplicabilitate nu mai este inexplicabilă.

Project Management-ul este cel mai elocvent exemplu de abordare științifică în domeniul securității naționale și desfășurarea de acțiuni strategice prin preluarea metodologiei și practicilor de lucru din mediul economic, mai specific vorbind, din zona managementului industrial. După prima jumătate a secolului XX, au fost elaborate noi practici de eficientizare a lucrului în echipă spre obținerea de performanță maximizată într-un proiect. Meritul acestor noi abordări îl constituie elaborarea de noi instrumente, mai logice, mai rafinate și suple din punct de vedere al gestionării procesului de creștere eficientă al unei organizații. Așadar, cum aminteam mai sus, strategia de securitate a României seamănă în mare parte cu o grila de project management. Ca parte introductiva, în strategia noastră de securitate regăsim: interese naționale, care coincid cu scopul unui proiect (proiectul fiind însăși strategia de securitate), regăsim obiectivele naționale, direcțiile de acțiune și principalele mijloace pentru asigurarea securității naționale a României. Dincolo de această dimensiune, un instrument de autoevaluare este analiza SWOT — specifică project managementului, unde evaluarea mediului de securitate, identificarea factorilor de risc din mediul intern și internațional, trebuie să țină cont de: *punctele tari* (atuuri, realizări naționale și regionale) și *punctele slabe* (vulnerabilități în plan intern ale unei națiuni), de *amenințări* (factorii de risc externi la adresa securității naționale) și *oportunități* (obiectivele corelate la tendințele României în mediul extern: internațional și regional)[137]. Acestea sunt doar premisele trasării strategiei naționale de securitate — sunt primele semne care reflectă starea de sănătate și potențiala direcție a unei națiuni.

[137] Punctele tari și punctele slabe reprezintă analiza mediului intern a națiunii în acest studiu de caz. Amenințările și oportunitățile țin de mediul extern și sunt evaluate ca atare.

În altă ordine de idei, avem nevoie de un proiect mai amplu ce presupune o strategie de implementare mai specifică, direcționată spre niveluri de responsabilitate și competență bine delimitate. Lipsa elementului de feedback creează probleme de repoziționare și flexibilizare permanentă în problematica securității naționale. Aceasta se realizează prin instrumente și centre de analiză bine specializate.

Project Managementul este însa, încă uzitat și eficient, dar nu suficient pentru nevoile actuale ale mediului de securitate. Este un instrument elaborat în perioada de industrializare majoră a acelor vremuri și deosebit de util pentru acest sector și tendințele caracteristice deceniilor trecute. Extinderea economicului spre sfera serviciilor a descoperit noi practici și proceduri de maximizare a eficienței proiectului în cadrul unei organizații.

Companiile au devenit mult mai flexibile la schimbările de pe piață, activitatea acestora este mult mai specifică, iar instrumentele folosite sunt tot mai variate. Competiția strânsă forțează organizațiile de toate tipurile să devină adaptabile la provocări într-un timp cât mai scurt. Această abordare nu presupune elaborarea de sisteme de lucru mai complicate, care ar îngreuna poziționarea pe scena concurențială, ci dimpotrivă, conceperea unor instrumente suple care pot fi adaptate la cultura organizației respective. Mediul de securitate impune ca elaborarea unor tehnici și practici de acest gen să conducă la rezultate concrete într-un timp record și cu resurse bine gestionate. Desigur, o modelare a sistemului intern în această direcție presupune o strategie dezvoltată, cel puțin, pe termen mediu.

Criza serviciilor de informații a fost în permanență rezultată din incapacitatea de a previziona și preîntâmpina incidente nedorite, sau mai bine spus, de ieșirea din starea de confort și normalitate a unei națiuni.

Un studiu elaborat în 1998 de către Consiliul pentru Relații Externe a SUA asupra îmbunătățirii *intelligence*-ului *național american*, arăta că: „Nevoia pentru intelligence și pentru o capabilitate la nivelul conducerii SUA de a colecta, produce și disemina rămâne critică. (...) În cele din urmă,

este important de reținut că nici o reproiectare sau reglementare nu poate compensa absența leadership-ului. Aceasta se va prăbuși pe actualii și viitorii *intelligence seniors* ai comunității informative, pe nevoia de produce dezvoltarea abilităților de management drept o prioritate, de a promova o cultură în care excelența este recompensată, talentul este dezvoltat, calitatea este valorificată, asumarea riscului legitimată să fie încurajată și respectul pentru lege de necontestat. Acestea, încredințate cu atenție sunt responsabile pentru cultivarea unui astfel de mediu"[138].

Același studiu arată că prioritizarea este o necesitate extremă. Nevoia de a izola *intelligence*-ul de presiunea politică este un real argument pentru a menține o puternică capabilitate centralizată și totodată de a nu lăsa *intelligence*-ul să dea naștere unor preocupări mai presus decât factorii politici decizionali și departamentali. Analizele competitive ale problematicilor controversate pot fi protejate de a fi politizate. Cea mai bună cale de a asigura analize de înaltă calitate este de a-i atrage pe cei mai buni analiști în proces. Aceasta ajută la dezvoltarea unei gândiri în termeni de competiție, drept una de îmbunătățire a personalului de carieră (reținerea personalului), dar și a fluxului de personal. Nu oricine trebuie să obțină o carieră cu o componentă de management. Aceasta nu înseamnă că sunt de neglijat pregătirile și abilitățile de management. Din contră, ultimele tendințe arată că serviciile de informații pun un accent particular pe formarea și dezvoltarea competențelor în management.

„... În fiecare dimineață în Africa, o gazelă se trezește. Ea știe că trebuie să fugă mai tare decât cel mai rapid leu sau va fi ucisă...

...În fiecare dimineață un leu se trezește. El știe că trebuie să depășească în viteză cea mai înceată dintre gazele, altfel va muri de foame.

---

[138] Maurice R. Greenberg, Richard N. Haass, *Making Intelligence Smarter*, în "Council on Foreign Relations', April 1998.

Nu contează ce ești, un leu sau o gazelă... când soarele răsare pe cer, ar fi mai bine să alergi"[139].

Pornind de la aserțiunea că mediul de securitate a devenit o scenă de competiție complexă și interdependentă, unul din conceptele cheie folosite și aplicate în managementul strategic este cel de *intelligence competitiv*, de altfel o tehnică și terminologie preluată din zona business-ului concurențial.

Transpus la nevoile strategice și tactice ale securității naționale, *intelligence*-ul *competitiv* este gândit și coordonat pe monitorizarea competitorilor, oriunde și oricare ar fi aceștia, într-un cadru specific de acțiune. Competitorii sunt acele persoane, organizații sau state pe care le consideram rivale intereselor și obiectivelor noastre, și cu care ne aflăm în competiție. *Intelligence*-ul *competitiv* presupune dealtfel stabilirea a ceea ce competitorii noștri vor face înainte de a acționa. Din punct de vedere strategic, putând previziona planurile unui competitor îți vei putea construi propria strategie de contracarare a planurilor acestuia. Așa cum ne putem aștepta, aceasta va implica mai multe metode tactice la nivelul de colectare a informației, dar de asemenea impune integrarea într-o infrastructura informațională, analiza și distribuirea informației, și în final, calcularea deciziilor pe baza informațiilor și a analizelor obținute. *Intelligence*-ul *competitiv* este ingredientul indispensabil al *strategiei competitive.*

Intelligence-ul *competitiv* este în general compus din cinci mari zone de încercare și trei abordări principale care se referă la cadrul de acțiune: determinarea strategiilor; percepțiile competitorului; eficiența operațiunilor curente; capabilitățile competitorului; prospectarea pe termen lung a mediului de acțiune[140].

Intelligence-ul *strategic* se preocupă de analiza competitorului sau dobândirea unei înțelegeri despre obiectivele viitoare ale competitorului, strategia actuală, presupuneri despre acesta și capabilitățile sale — componente diagnostic;

---

[139] Aurora WDC, motto, home page, http://www.aurora.com.

[140] *Arik R. Johnson*, Managing Director of the CI consultancy Aurora WDC, workpaper, 2004.

informație despre mediul său de acțiune (parteneri, dezvoltare, etc.).

Intelligence-ul *tactic* este în general operațional și la o scară mult mai mică, nu atât de centrat pe a fi predictiv. Problematicile tactice presupun informații despre politicile și planurile de zi cu zi ale competitorului.

Contra intelligence-ul presupune protejarea secretelor organizației. De obicei presupune securizarea informației și a tehnologiei utilizate, a strategiilor și planurilor de acțiune.

CICLUL INTELLIGENCE-*ULUI COMPETITIV*

CIA descrie ciclul informațional ca fiind: „procesul prin care informația brută (neprelucrată) este obținută, culeasă, transmisă, evaluată, analizată și pusă la dispoziție, ca piesă de *intelligence*, pentru a fi folosită și pusă în acțiune de către factorii decizionali politici". Aici avem cinci pași care constituie acest ciclu: planificare și direcționare; colectare și cercetare; procesare și stocare; analiză și producție; diseminare și livrare.

Adevărata valoare a *intelligence*-ului competitiv este de a asigura instrumente organizaționale de identificare a ceea ce va face competitorul, nu despre ceea ce competitorul a făcut deja.

Pe scurt, o etapă primară a Intelligence-ului Competitiv o reprezintă scanarea mediului cu implicarea pașilor mai sus enunțați.

Astăzi, operațiunile de intelligence trebuie să acopere a gamă foarte largă de amenințări și nevoi politice, mai multe decât oricând, și să lucreze foarte strâns alături de factorii decidenți. „Trebuie acordată o înaltă prioritate asupra conservării și sporirii acestor colectări de intelligence și capabilităților analitice care pot furniza informație despre amenințări reale la adresa securității naționale"[141].

[141] A National Security Strategy for A New Century, NSC studies, May 1997.

Sprijinul *intelligence*-ului este necesar în dezvoltarea și implementarea politicilor naționale de toate tipurile. Fuziunea dintre toate ramurile *intelligence*-ului poate furniza cea mai eficientă colectare și analiză de date pe aceste subiecte.

Trecerea de la *complicat* la *complex* impune o dezvoltare accentuată a colaborărilor, tot astfel, posibilitatea de acțiune cât și cea de interacțiune a celor implicați în proces, au cunoscut și ele mutații semnificative, spre autonomizarea deciziei. Tocmai de aceea, actorii strategici devin tot mai numeroși, nu mai există un singur personaj principal și devine necesară negocierea; ceea ce necesită și multiplică procesele de implicare și cooptare, de motivare a întregului personal, care astfel este pus extrem de frecvent în situații comunicaționale, pentru a putea lucra împreuna în echipe, pentru a face schimb de experiență, pentru a învăța.

Unii cercetători consideră necesară utilizarea întregii *„inteligențe organizaționale"*[142] necesitând punerea efectivă în valoare a potențialului intern. Prin aceasta înțelegem valorificarea (cu ajutorul tehnologiilor informatice și comunicaționale) cunoștințelor angajaților — este vorba de cunoștințe puse în comun. Scopul este de a construi cele mai bune variante de utilizare a resurselor de care organizația dispune, conform obiectivelor care de asemenea, dată fiind fluiditatea evoluțiilor interne și externe organizației, vor trebui și ele ajustate în mod dinamic.

Este vorba, în acest sens, tocmai de *adaptare* și *asimilare*, care sunt cele două caracteristici esențiale ale comportamentului inteligent. Daca mediul extern este cel care impune necesitatea unui comportament inteligent, valorificarea la maximum a mediului intern se va baza tocmai pe sinergiile între uman și artificial. Iată considerentele în baza cărora putem pleda pentru modelul organizației inteligente.

Caracteristicile în definirea acestui model, adaptabil la mediul de securitate, le putem identifica după cum urmează:

---

[142] Robert Salmon, Yolaine de Linares, *„L'intelligence compétitive; une combinaison subtile pour gagner ensemble"*, în „Economica", Paris, 1997.

orientarea către factorul decident; preocuparea pentru veghea de securitate și benchmarking (sau etalonajul competitiv); proactivitatea (capacitatea de a-și provoca viitorul, „devenirea") și totodată agilitatea (capacitatea de a reacționa mai rapid decât concurenții); inițierea de proiecte de organizație (capabile să reunească inițiativele ansamblului de personal); utilizarea rețelelor inteligente cooperative (care să mobilizeze inteligențele atât umane cât și artificiale); virtualizarea organizației (care astfel ia contururi tot mai vagi, care devine omniprezentă în spațiu și timp — cu ajutorul tehnologiilor de comunicații, ale cărei angajați formează și deformează echipe de proiect cu o mobilitate foarte mare, prin punerea în comun a cunoștințelor și valorizarea competențelor lor).

„Dacă-ți cunoști dușmanul și te cunoști și pe tine însuți, nu trebuie să-ți fie frică de rezultatul a o sută de războaie" (Sun Tzu — 500 î. Hh).

„Benchmarking-ul este un proces de măsurare continuă și sistematică și de comparare a procesului de desfășurare a activității unei organizații cu cel al unor lideri, indiferent în ce parte a lumii s-ar afla, în vederea obținerii de informații care să-i permită organizației respective să acționeze pentru îmbunătățirea performanțelor sale"[143].

De unde vine conceptul de „benchmarking competitiv"? Primul demers structurat a apărut în 1979 la firma Xerox, care s-a confruntat cu atacurile continue din partea concurenților ei japonezi. Liderul mondial în fotocopiatoare a reacționat prin analiza detaliată a mașinilor de la concurență cu scopul de a-i reduce propriile costuri de producție

Există 4 tipuri de benchmarking definite în modul următor: *Benchmarking intern* — compararea la același tip de operații cu altele similare din aceeași organizație (între centre, între țări); *Benchmarking concurențial* — compararea specifică cu concurenții asupra produsului, metodei, proceselor. Pentru acest tip de comparație între două organizații direct concurente, foarte des, apare dificultatea de a obține informații — mai ales în Europa); *Benchmarking funcțional* —

[143] Sarah, Cook, *Practical Benchmarking*, London, 1997.

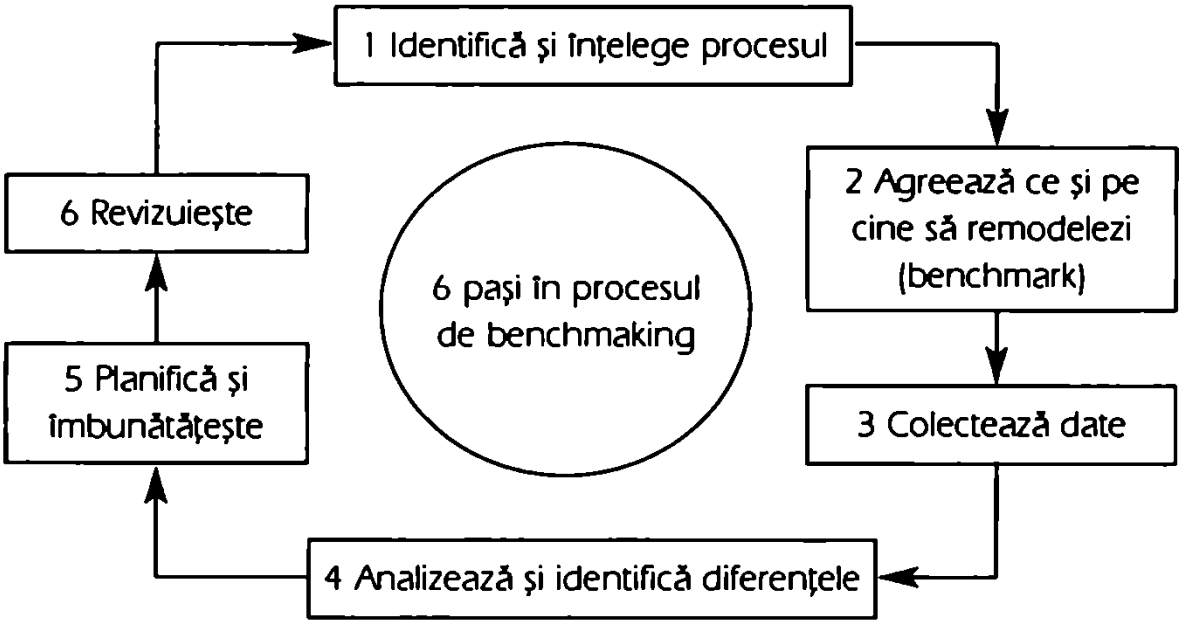
compararea funcțiilor similare între organizații care nu sunt concurente din același sector de activitate pentru decelarea de tehnici novatoare; *Benchmarking generic* — compararea între organizații din sectoare diferite asupra proceselor sau metodelor de lucru. Un informatician poate de exemplu, să compare funcția sa de logistică cu același tip de funcție din sectorul de distribuție.

În practică, demersurile funcționale și generice se arată a fi cele mai ușor de aplicat deoarece concurența nu intră în calcul. Punerea benchmarking-ului în implementare implică și o anumită stare de spirit, o anumită „umilință" față de punerea în cauză a propriilor practici, o atitudine față de schimbare, o deschidere față de ideile noi, față de creativitate, a inovării în aplicarea procedurilor existente.

În fine, pentru buna sa derulare presupune un „cod de conduită" cum ar fi confidențialitate și reciprocitate față de schimbul de informații. Concret, căutarea de „bune practici" (*vezi figura de la pagina următoare*) necesită timp și mai multe căi disponibile: surse interne (biblioteci, reviste, publicații, servicii interne) și externe (ONG-uri, publicații, seminarii, surse universitare, etc.). Dar, remodelează de asemenea și terenul: returnarea de informații clientelei, anchete telefonice, vizite la sediu sau investigații mai speciale, rețele, consultanți.

Un alt concept specific ariei de maximizare a eficienței unei organizații este „reengineering-ul" care promovează ideea că „în lumea de azi, care aparține clienților (de securitate — în cazul nostru[144]), concurenței și schimbării, a te organiza pe bază de operații separate este depășit. Organizațiile trebuie să își organizeze activitatea pe bază de

[144] În raportul *Reinventing Government / Creating a Government that Works Better and Costs Less — Reinventing Support Services* (1993/1997), proiect conceput de echipa de analiști a vice-președintelui SUA la acea vreme, Al Gore, în capitolul *The Intelligence Community, INTEL 02: Enhance Community Responsiveness to Customers*, clienții de securitate ai comunității informative sunt numiți: decidenții politici, militari, civili, strategici și tactici.


1 Identifică și înțelege procesul
2 Agreează ce și pe cine să remodelezi (benchmark)
3 Colectează date
4 Analizează și identifică diferențele
5 Planifică și îmbunătățește
6 Revizuiește
6 pași în procesul de benchmaking

procese". Ce desemnează „procesul"? „Un ansamblu de activități care, împreună, produc un rezultat care are valoare pentru client — de exemplu dezvoltarea unui produs"[145] Hammer & Champy, (strategie, politică de securitate, instrument, instituție, corp de acțiune și/sau combatere).

Desigur, conceptele prezentate par foarte atractive, este important ca ele să fie adaptate și implementate la specificul, necesarul și cultura fiecărei organizații. În cazul nostru, reengineering-ul este potrivit când realizăm că: ***MAI MULTE POSTURI SUNT COMBINATE ÎNTR-UNUL SINGUR (SE CONSTRUIESC PROCESE INTEGRATE); PROCESELE AU VERSIUNI MULTIPLE; LUCRĂRILE SE EXECUTĂ ACOLO UNDE ESTE MAI NORMAL (RIGIDITATEA REȚELEI IERARHICE SE REDUCE CONSIDERABIL ÎN ANUMITE CAZURI); ESTE ESENȚIALĂ INIȚIATIVA, RESPONSABILITATEA ȘI COMPETENȚA, NECONCORDANȚELE SUNT REDUSE LA MINIMUM, PREVALEAZĂ OPERAȚIILE HIBRIDE: CENTRALIZAT/ DESCENTRALIZAT.***

Toate acestea pot fi implementate și susținute de specialiști în managementul schimbării prin trasarea unor strategii pe termen mediu și dezvoltarea de centre sau nuclee

[145] Hammer & Champy, *Reengineering*, 1993/1996, p. 52, 27.

analitico-pragmatice bine specializate pe problematici cu caracter specific.

În analiza procesului de benchmarking guvernamental și de securitate (pentru că cele două domenii coexistă și se completează reciproc) al Statelor Unite, în 1997, o echipă de consilieri ai vicepreședintelui Al Gore au dezvoltat un raport și o strategie ipotetică racordate la tendințele actuale concurențiale, ce pune în ordine 15 priorități strategice ale națiunii americane. Acestea sunt:

Leadership-ul	Parteneriatele	Noile Tehnologii
Comunicarea și Comunicațiile	Managementul Financiar	Re-engineering-ul & Direcționarea
Concentrarea pe Nevoile Clientului	Procurarea & Achizițiile	Dezvoltarea Resurselor Umane
Inovație & Educație	Planificare Strategică & Măsurarea Performanțelor	Suportul Legislativ
Designul Organizațional	Stimularea Echipelor (în sens de împuternicire)	Servicii Administrative

Abordarea arată cât se poate de normal din punctul meu de vedere. În momentul în care vorbim de leadership, nu putem să nu ne întrebăm cum se produce managementul schimbării. Astfel, o strategie care cuprinde domenii și elemente prezentate mai sus, trebuie să previzioneze viitorul unei națiuni pe 5–10 ani, sau cel puțin, obiectivele strategice și așteptările dezvoltate într-o formulă mai concretă pe un segment de timp determinat.

Retrospectiva Performanței Naționale a celor 15 categorii a fost elaborată în ideea conceperii unui instrument pentru implementarea și îndrumarea schimbărilor strategice, numită de către „proiectanți" — *reinventarea guvernării.*

Dificultatea de a răspunde la întrebarea: „unde mă (re)găsesc după 5–10 ani?", provine din incapacitatea de leadership. Leadership-ul eficient ar trebui întreținut, cultivat și alimen-

tat prin informație, analiză și inovație (analiști și implementatori strategici), prin dezvoltarea unei clase politice și civice educate în spiritul eticii naționale și a competiției coerente.

Un instrument, deja cunoscut și implementat la nivelul factorilor decizionali occidentali este *WarRoom*-ul *strategic*. Un *WarRoom strategic* analizează în timp real starea de sănătate a unei națiuni pe mai multe dimensiuni (arii de analiză) cum ar fi: economic, militar, social, imagine, politică externă, intangibil, etc. Aș dori să mă refer la zona valorilor intangibile care este cea mai sensibilă, dar care, capacitată strategic, poate deveni cea mai eficientă componentă de dezvoltare a unei națiuni. Indicatorii folosiți sunt mai speciali, ei se referă la cetățenii națiunii și la tipul lor de reacție în anumite situații. Acești indicatori se măsoară cu instrumente specifice și includ: credințele naționale, capacitatea motivațională a cetățenilor la un moment dat, grade și nișe de acceptabilitate, poziția față de un anumit incident național, internațional sau local — fie acesta o politică sau strategie adoptată de către stat.

Pentru a realiza un astfel de proiect avem nevoie de un *radar de securitate* împânzit pe teritoriul geografic și administrativ al țării, compus din centre de analiză proprii, centre (laboratoare) de analiză și sondare universitare, institute de cercetare și ONG-uri (*think-tank*-uri de profil specializate). Dintr-un alt unghi de vedere, consider că starea de securitate a unei națiuni este dată atât de analiza mediului intern, a celui extern, cât și a interdependențelor dintre cele două. Așadar, analiza mediului intern conferă acea bază de cunoaștere și instrumentare care ne poate reda orizontul strategic național pentru circa 5–10 ani, definind capacitățile naționale. Un *WarRoom Strategic* susținut de un *radar de securitate* poate deveni procesorul principal pentru elaborarea căilor de implementare a politicilor publice și strategiilor de dezvoltarea, asigurarea și controlul nevoii de securitate.

Pentru a susține împlinirea calitativă a acestui proiect trebuie găsită soluția pentru asigurarea eficienței decizionale. Combinația unui sistem de coordonare mixt de tip centralizat-descentralizat pare, din punctul meu de vedere, cea mai

justă. Această schemă propune existența unui *Consiliu Național de Securitate* sub comandă unică ce are atribuții în desemnarea liniilor generale strategice, preluarea gestionării naționale în situații de criză majoră și aprobarea misiunilor (de anvergură) cu caracter special. La nivel acțional zilnic (analiză și operativ), pe această schemă, se interpune, formând o structură matriceală, aportul fiecărui serviciu de informații în parte, pe problemele sale specifice — astfel se va evita atribuirea unicei soluții acceptate de către un *Consiliu Național de Securitate* pentru rezolvarea problemelor apărute. Mai multe căi de abordare și acțiune reprezintă mai multe șanse de reușită, mai multă valoare adăugată și câștig de know-how. Desigur, aceasta este o abordare reducționistă, o soluție imaginară care necesită viziune, spirit novator și atitudine. Ideea de la care am pornit se referea la faptul că un centru unic de coordonare sau comandă poate să nu adopte cea mai bună cale de rezolvare a unei probleme — fiind doar una general agreată. Totodată, suprapunerea mai multor centri decizionali și acționali la nivelul serviciilor de informații pot complica activitatea acestora și diminua eficacitatea. În concluzie, trebuie găsită o soluție mixtă care să excludă două potențiale riscuri.

Strategia de Securitate Națională a României este din punctul meu de vedere incompletă în acest moment; acestui proiect îi lipsește explicit programul și strategia concretă de implementare, căile și instrumentele folosite pentru atingerea obiectivelor într-o formulă mult mai amplă, chiar și ca a doua foaie, dincolo de interfața prezentată publicului.

Într-unul din discursurile sale, Chris Donnelly — consilier pentru Europa Centrală și de Est al fostului secretar general al NATO, mesaj intitulat sugestiv: *„Security in the 21st century: new challenges and new response"*, acesta identifică trei factori principali care au cel mai mare impact asupra actualei scene de securitate: proliferarea de tehnologie necontrolabilă; creșterea diferențelor dintre statele bogate și sărace; revoluția informatică.

Din acest punct de vedere, trebuie să reconsiderăm ce constituie starea de securitate astăzi, care sunt amenințările

la securitate și care ar trebui să fie răspunsurile noastre la aceste amenințări.

Cu un deceniu în urmă, termenul de „securitate națională" era sinonim cu termenul de „apărare". Astăzi, pentru majoritatea statelor euro-atlantice, securitatea este măsurată mai întâi în termeni nemilitari, iar amenințările care primează sunt de natură nemilitară. Aceste amenințări includ: guvernarea incompetentă, corupția, crima organizată, insecuritatea granițelor, traficul și comerțul ilegal (arme, droguri, contrabandă, persoane), migrația ilegală, conflictul etnic și religios, proliferarea armelor de distrugere în masă, diminuarea resurselor naturale, ca de exemplu apa și desigur terorismul.

Human Development Report dă două înțelesuri principale conceptului de securitate individuală: „înseamnă, în primul rând, siguranța față de amenințări cronice precum foametea, bolile și constrângerea. În al doilea rând, înseamnă protecția față de modificările bruște și dureroase în modelele vieții de zi cu zi — fie acasă, fie la muncă sau fie în comunitate. Aceste amenințări pot exista la toate nivelele de venituri și dezvoltare națională"[146].

De asemenea, circumscrie și șapte dimensiuni ale securității individuale[147]: securitate economică; securitatea hranei; securitatea sănătății; securitatea mediului; securitate personală; securitatea comunității; securitatea politică.

Conceptul de Reforma Sectorului Securității este relativ nou în teoria și practica relațiilor internaționale și poate fi folosit ca instrument novator și folositor la întărirea democrației și la dezvoltarea social-economică. Conceptul cunoaște o dezvoltare constantă și complexă.

Studiul interdisciplinar este singura cale de a analiza inter-relațiile dintre variatele instituții ale sectorului de securitate națională, dintre acestea și societatea civilă. Democratizarea acestor instituții necesită măsuri specifice legale,

——— [146] United Nations Development Programme (UNDP), Human Development Report, 1994, New York: Oxford University Press, p. 23.

[147] *Ibidem.*

organizaționale, educaționale și politice. Contextul geopolitic, economic, cultural și istoric al reformei sistemului de securitate este decisiv pentru modul în care este programată și aplicată[148].

„Nici o societate nu poate exista dacă nu simte nevoia de a afirma și reafirma la intervale regulate sentimentele și ideile colective ce constituie unitatea și personalitatea acesteia. Această reconstituire morală nu poate fi realizată decât pe baza reuniunilor, ședințelor și mitingurilor în cadrul cărora indivizii, fiind solidari unii cu ceilalți, își afirmă în comun sentimentele comune; ca rezultat avem de a face cu ceremonii care nu se deosebesc de ceremoniile religioase obișnuite, fie ca gen de obiectiv, adică rezultatul obținut, fie prin procedură aleasă în vederea obținerii unui astfel de rezultat"[149].

Pentru a gestiona cu eficiență maximă aceste probleme, care în mod contrar, pot genera frustrări naționale, este imperios necesar instituirea unui parteneriat cu entități credibile și capabile să transmită și să propage mesaje și percepții obiective la nivelul sectorului civil vis-a-vis de problematica de securitate — inclusiv dezvoltarea unei culturi de securitate.

Aceste strategii au un rol foarte important și sunt implementate prin dezvoltarea instituției lobby-ului, dezvoltarea parteneriatelor cu ONG-uri de profil, mass-media, universități (prin departamentele sale specializate în domeniul studiilor de securitate), angajarea formatorilor de opinie într-un astfel de proces.

„ONG-urile pot deveni forța majoră în această ecuație. Pentru aceasta, ONG-urile vor trebui să-și organizeze și

---

[148] Andrzej Karkoszka, *Security Sector Reform - the Concept. Its Political Usefulness and Growing Importance*, în "Studies in Contemporary History and Security Policy", vol. 12.

[149] P.R Calder, *Ritualization in international relations. Philosophical Transactions of the Royal Society*, 1966, series: B, 251:451–56. Autorul vorbește despre despre folosirea simbolurilor de identitate în ritualizarea războiului.

articuleze mesajele proactive mult mai bine, alianțele ONG dintre rețelele Nord-Sud vor crește ca număr și forță. Alianțele strategice cu media vor fi cruciale. Încurajarea populației prin informare va fi o adevărată provocare pentru majoritatea guvernelor; cu cât mai bine informată și coordonată, societatea civilă va pretinde mai mult de la guvernare cât și de la companiile private". Aceasta este viziunea Consiliului Național de Intelligence al SUA pentru anul 2015[150].

Iată și câteva argumente pentru un parteneriat cu ONG-uri specializate: ONG-urile sunt excelenți formatori de opinie, gestionează și promovează o imagine în comunitate, poate modela percepții — o dimensiune intangibilă; ONG-urile încurajează participarea și inițiativa — valorile unei societăți democratice sănătoase; ONG-urile se pot constitui în instituții sau grupuri de lobby — pot deveni un suport în atingerea obiectivelor de interes național; ONG-urile au o arie de expertiză specifică relativ bine dezvoltată — orientată pe un domeniu concret (mai ușor de conceput o strategie pe termen mediu) — caracterizate prin elaborare și implementare de proiecte, capacitate de a atrage și capitaliza resurse de toate tipurile; ONG-urile pot fi suport pentru decision-making prin oferirea de soluții, studii, cercetări, asistență, consiliere, etc.; ONG-urile privite ca sursă de stabilitate și securitate — creează un efect de feedback și control la nivelul societății în ansamblu sau pe anumite comunități — grupuri țintă; ONG-urile au un rol major în extinderea granițelor, a cooperărilor și parteneriatelor internaționale.

„... Mai degrabă, organizațiile trebuie să-și aleagă măsurătorile de performanțe ce pot ajuta la descrierea eficienței organizaționale, a direcției și realizărilor; apoi să le folosească

——— [150] ECSP REPORT · ISSUE 7, *The U.S. National Intelligence Council's Global Trends 2015: Excerpts, Commentaries, and Response*, January 2001.

[151] *Serving The American Public: Best Practices in Performance Measurement*, în "Benchmarking Study Report", June 1997.

agresiv la îmbunătățirea produselor și serviciilor pentru clienții și beneficiarii"[151] de securitate.

Dacă agreăm ideea că starea de securitate se realizează pe mai multe dimensiuni și indicatorii folosiți nu sunt doar de factură militară, atunci voi sugera ca strategia de colaborare dintre instituțiile de securitate ale statului și reprezentanți ai societății civile să cuprindă un cadru mult mai larg de acțiune. Dacă vom ajunge la concluzia că asigurarea unui cadru pentru dezvoltarea prin educație formală și non-formală a tinerilor din România este un obiectiv strategic, sau securitatea mediului este o prioritate în acest domeniu, atunci este imperios necesar ca puntea de legătură să nu fie constituită doar prin și cu ONG-uri care organizează mese rotunde și conferințe despre starea de securitate a națiunii, ci și cu acele entități ale societății civile care au un puternic potențial implementator. Revin la una dintre caracteristicile ONG-urilor enunțate mai sus și întăresc argumentul meu: ONG-urile au o arie de expertiză specifică, relativ bine dezvoltată — orientată pe un domeniu concret (mai ușor de conceput o strategie pe termen mediu) — caracterizate prin elaborare și implementare de proiecte, capacitate de a atrage și capitaliza resurse de toate tipurile.

Mai mult, colaborarea cu un cerc foarte strâns de ONG-uri (4–5 la număr), poate induce un grad de susceptibilitate, dezvoltându-se ideea că există un grup mic de actori ce duc o politică direcționată — risc de contra-imagine. Desigur, e nevoie de identificarea unor lideri ai societății civile care pot implementa eficient anumite proiecte, pot transmite valori și idei la nivelul cetățeanului, pot face lobby pozitiv României, pot reda credibilitatea partenerilor (instituțiile de securitate) în societate, și de ce nu, în cele din urmă se pot constitui în sursă de stabilitate și securitate națională.

Este important să propagăm valorile Trans-atlantice și să ne concentrăm eforturile pentru integrarea României în UE, dar cred, că mai întâi trebuie să fim îndreptați către satisfacerea nevoilor naționale conjugate desigur cu cele mai sus enunțate. Mai sunt și vor fi multe probleme de rezolvat;

lipsa de viziune, de pragmatism și de implementatori ne vor reduce semnificativ orizontul politic și economic. Nu trebuie să așteptăm ani pentru a prelua modele și practici testate de alți parteneri, trebuie să ne dovedim leadership-ul și să acționăm energic pentru a satisface nevoile acestei națiuni, adaptate la specificul și credințele noastre.

TINERII ŞI EDUCAŢIA PENTRU SIGURANŢĂ NAŢIONALĂ

Cristian Rizea

Trăim o perioada ce își va pune cu siguranță amprenta asupra societății românești pentru o foarte lungă perioadă de timp de acum înainte. După o importantă realizare diplomatică și militară și aici mă refer la calitatea de membru al Alianței Nord-Atlantice ne așteaptă în următoarele zile o manifestare cu adevărat istorică: participarea cu drepturi depline la cel mai înalt nivel al Alianței la un summit cu dreptul de a participa la procesul decizional.

În calitate de membru NATO vom beneficia de „oxigenul" stabilității, propice unei dezvoltări economice durabile. Securitatea oferită de Alianță este mai ieftină și mai profitabilă decât cea dinainte de 1989 și mai solidă ca niciodată.

Beneficiile nu vor veni imediat, nu în masă și nu automat. Siguranța investițiilor străine depinde și de calitatea mediului de afaceri dar este și influențată de NATO, iar efectele în acest plan vor apărea pe termen mediu și lung. În mod cert, însă, vom cumpăra o pace teritorială și politică la cel mai bun raport calitate — preț.

Noile tehnologii, turismul, construcțiile, infrastructura, industria textilă, dar și cea din domeniul producției militare sunt domeniile care, în prima fază, vor avea de câștigat din aderarea României la NATO. Creșterile nu vor veni neapărat din majorarea volumului investițional, ci în mare parte de pe urma *outsourcing*-ului, adică din faptul că foarte multe companii românești vor deveni sub-furnizori pentru producătorii mondiali. Se va ușura accesul la foarte multe fonduri din partea organismelor financiare internaționale, iar valorile activelor firmelor românești vor crește cu 10% — 50%.

„Reformele în domeniul militar, economic, legislativ și administrativ vor continua fără preget până la integrarea deplină a României în Alianță. Cu toate acestea, pentru noi aderarea la NATO nu reprezintă un scop în sine; acest lucru

reprezintă începutul reintegrării noastre în comunitatea de valori ăi practici occidentale. Suntem conștienți că și după aderare, reformele militare trebuie să continue și să fie însoțite de creștere economică, de o luptă eficientă împotriva corupției, de consolidarea statului de drept"[152].

„Pe termen scurt aderarea la NATO ar putea aduce dividende politice importante care se vor răsfrânge și în sectorul economic. Dintr-o perspectivă economică, se poate spune că efectele aderării la Alianța Nord —Atlantică echivalează cu un triplu A politic. Nu trebuie neglijat nici faptul că, în procesul aderării România își va asuma angajamente concrete privind reformele administrative și economice, care vor veni în sprijinul procesului de integrare în Uniunea Europeană. La rândul său, procesul de pregătire a integrării în UE va amplifica consecințele pozitive pe care aderarea la NATO le va avea asupra mediului social și economic românesc" (Mircea Geoană).

Dar NATO nu mai reprezintă doar o alianță militară. Rolul său politic a luat o amploare foarte mare în ultimii ani. Și putem vorbi și de influența economică pe care o are Alianța, în mod direct sau prin intermediul calității de membru. Integrarea se va face nu doar la nivel de forțe armate, integrarea se va face în toate segmentele societății, putem observa zonele de interes ale Alianței din însăți Tratatul de bază ce consfințește amplificarea schimburilor comerciale între parteneri atât în sfera industriei de apărare cât și în terțe domenii. Alianța are de asemenea comitete ce se ocupă de promovarea noilor tehnologii, a programelor de cercetare și dezvoltare. Dar în primul rând calitate de membru NATO ne face părtași la grupul select ce stabilește și controlează noul mediu de securitate, și direcțiile dezvoltării viitoare.

Pe de altă parte, Uniunea Europeană este principalul partener economic al României. Viitoarea aderare a țării noastre la Uniunea Europeana ne va deschide porțile celei mai mari piețe economice libere a planetei, va da posibilitatea forței de muncă românești să se adapteze la cerințele unei

[152] Adrian Năstase. *Alocuțiune la Institutul Nobel*, Oslo, 2002.

concurențe directe și bineînțeles și la câștiguri salariale comparabile cu actualele țări membre. Va fi o modernizare obligatorie, ca o condiție a supraviețuirii.

Uniunea Europeană este un laborator, o globalizare experimentală ce reprezintă pentru noi o șansă. O șansă deoarece ne pune la dispoziție un set de reguli comune, sprijin logistic și financiar, fonduri ne-rambursabile pentru restructurare, ceea ce constituie o practică în vederea integrării in viitoarea lume globală.

Prin încheierea Acordului de asociere la Uniunea Europeană, România s-a angajat ireversibil pe calea integrării europene. Strategia națională de pregătire a aderării României la UE, adoptată la Snagov, în iunie 1995, a jalonat etapele procedurale și acțiunile ce urmau a fi întreprinse în procesul de apropiere de structurile comunitare.

Uniunea Europeană constituie un cadru destinat să faciliteze statelor membre realizarea obiectivelor de politică externă și internă, cu respectarea și aplicarea consecventă a unor principii fundamentale comune, pe care România și le asumă în totalitate: principiul statului de drept și al respectării legii, cu stabilirea unui sistem legislativ uniform și asigurarea protecției drepturilor derivând din reglementările comunitare; principiul respectării drepturilor și libertăților fundamentale ale omului — norma juridică având valoare universală; principiul statului social; principiul pluralismului cultural; principiul subsidiarității.

„Mărimea pieței interne a acestei mari unități continentale cum este Europa, performanțele economice, stabilitatea și tăria monedei comune, competitivitatea, abilitatea de a folosi noile tehnologii, coeziunea socială, stabilitatea internă sunt, alături de influența politică și puterea militară, elemente esențiale în competiția la nivel global. Europa are în acest moment, o oportunitate unică de a deveni lider și formator al acestui proces de globalizare, oferind celorlați valorile sale democratice, modelul său social și cultural. Pe cont propriu, singur, nici un popor nu poate rezista globalizarii, nici măcar dacă liderii și reprezentanții săi ar nutri un maso-

chism devorant"[153]. În aceste condiții este de o importanță covârșitoare dezvoltare a noi concepte de parteneriat bazate pe binoumul autoritate–cetățean, de diseminare a informațiilor și a experiențelor positive.

Am ales un segment pe care îl consider extrem de important — *tinerii*. Ei sunt viitorul, vor locui, munci și crea într-o societate nouă. Dar viitorul nu aduce doar plusuri, odată cu noul statut dobândit de România apar avantajele dar și amenințările. În acest context trebuie să fim pregătiți pentru a reacționa dar mai ales trebuie să fim proactivi, trebuie să asigurăm acele cunoștințe care să genereze reacțiile care să diminueze costurile și pierderile.

PROBLEMA

O trecere în revistă a curriculei, începând cu clasa a V-a și terminând cu ultimul an de liceu, relevă un fapt îngrijorător: din educația tinerilor lipsește educația pentru siguranță națională. Lipsește cu desăvârșire chiar și din tematica orelor de dirigenție, aceasta în contextul în care țări extrem de bine situate din punct de vedere militar, economic și al poziției internaționale acordă o deosebită importanță formării unei atitudini sănătoase, vis-a-vis de siguranța națională a viitorilor cetățeni.

În România, instituțiile de siguranță națională sunt, din nefericire, extrem de puțin vizibile, iar informația cu privire la ele ajunge în lumea civilă diluată, adesea deformată. Sau nu ajunge. Câți dintre funcționarii publici, spre exemplu, cunosc organigrama SRI-ului? Sau pe cea a SIE? Câți știu care este obiectul de activitate al STS? Credem că nu mai e nevoie să aducem argumente în sprijinul ideii că este nevoie de crearea unei imagini unitare, obiective (nu favorabile, obiective) a românilor despre sistemul de siguranță națională al propriei țări. Sistem pe care, de altfel, cetățenii îl stipen-

——— [153] Ion Iliescu, *Integrare și globalizare. Viziunea românească*, Editura Presa Națională, București, 2003.

diază, dar pe care cei mai mulți îl denigrează ori de câte ori au ocazia.

Prin urmare, *este nevoie de educație pentru siguranța națională.* Cui vom adresa cu bune rezultate un asemenea demers? Evident, tinerilor, pentru că ei sunt categoria cea mai deschisă la minte și mai cu seamă pentru că lor le aparține viitorul acestei țări despre a cărei siguranță națională facem vorbire.

SOLUȚII POSIBILE

Trei ar fi variantele de rezolvare a problemei. Mai întâi s-ar putea introduce o disciplină de specialitate în curricula școlară. Apoi ar fi distribuirea unor materiale scrise - broșuri, pliante, CD-uri cu filme documentare etc. A treia posibil - soluție: susținerea unor serii de prelegeri cu tematica din aria de interes și, totodată, organizarea unor cursuri de scurtă durată (tip școală de vară) pentru cei interesați.

Desigur, mai pot fi găsite și alte soluții dar, în instanța ultimă, demersul nostru își propune să găsească o rezolvare viabilă, nu să inventarieze toate posibilele răspunsuri ale întrebării. Așadar, să analizăm variantele prezentate.

Introducerea unei discipline de studiu în programa școlară are câteva dezavantaje mari. Ca orice materie (aceasta s-ar putea numi, de exemplu, „Bazele siguranței naționale"), aceasta va trebui notată. Elevii vor trebui să parcurgă o serie de etape de verificare a cunoștințelor. Asta înseamnă învățat, lucrări, teste de evaluare, eventual teme de făcut. Pentru majoritatea elevilor o astfel de abordare „treadiționalistă" este puțin dezirabilă și riscă să construiască mai mult resentimente decât opinii favorabile. Pe de altă parte, o disciplină de studiu presupune cheltuieli — salariile profesorilor, manuale, alte materiale didactice. La nivel național suma nu ar fi de neglijat.

Diseminarea unor materiale scrise și audio-vizuale — a doua soluție propusă — s-ar putea să se înscrie în paradigma „muncă în zadar". Ce garantează că, odată distribuite, aceste

materiale nu vor fi ignorate sau, mai rău, aruncate la coș? Credem, răspunsul e cât se poate de clar.

Ultima soluție pare mai eficientă și asupra ei ne vom apleca în cercetarea ce urmează să o întreprindem. Serii de prelegeri cu privire la sensibilul domeniu al siguranței naționale au avantajul că, prezentate alert și atractiv, vor stârni interes și, în unele cazuri, dorința de a studia problema. Acest lucru ar urma să fie posibil prin organizarea de cursuri de scurtă durata. Asemenea cursuri ar putea deveni, la un moment dat, creuzetul unor idei noi, benefice în construirea domeniului. Totul s-ar putea face pe banii societății civile, prin programe rulate de organizații ne-guvernamentale de tineret. Acestea ar urma să structureze un sistem de educare și informare pe linia siguranței naționale. Evident, serviciile de siguranță ar trebui să contribuie la proiect prin furnizarea unor specialiști care să cristalizeze temele de discutat.

În acest sens, proiectul pe care îl propun se va materializa într-o primă etapă în parteneriatul dintre o autoritate guvernamentală, cu un puternic și bine conturat rol în sprijinirea activităților tinerilor și în promovarea activităților de educație ne-formală, și aici mă refer la Agenția Națională pentru sprijinirea inițiativelor tinerilor și Asociația Absolvenților Colegiului Superior de Siguranță Națională, „PAIDEIA", o organizație ne-guvernamentală cu o acoperire și expertiză excelente pe domeniul siguranței naționale.

Astfel, în cadrul Universității de vară, două module vor fi gestionate de Asociație, în cadrul acestora punîndu-se în discuție teme ca: valori europene și euro-atlantice, cetățenie europeană, poziția României în noul context — membră a NATO o alianță politico-militară cu o implicare tot mai puternică în asigurarea stabilității și ordinii la nivel global și în calitate de candidat la integrarea în UE. Acest program ce se adresează tinerilor cu rezultate deosebite la învatatură poate deveni un adevărat creuzet pentru viitorii cetățeni ai Europei, liderii de mâine ai țării noastre. Am pornit acest proiect de la constatarea că în ecuația asigurării siguranței naționale avem binomul *autoritate–cetățean*. Noile condiții ale mediului internațional tot mai fluide și neprevăzute, în

care România este un actor cu drepturi depline, fac din funcționarea relației autoritate–cetățean, la nivel maxim, o necesitate. Prin reformă și restructurare, autoritatea se adaptează și se pliază noilor tipare, astfel încât pentru un randament superior este necesară o scară de valori comune, un limbaj comun care să reducă la minimum pierderile datorate neînțelegerii. Limbaj se poate construi prin aceste programe de educație ne-formală cu aportul organizațiilor ne-guvernamentale implicate civic. Nu merg până la întrebarea pe care John Fishgerald Kenedy o propunea tuturor americanilor în anii '60: „nu te întreba ce poate face țara pentru tine ci ce poți face tu pentru țară".

Venim pentru început cu acest proiect ce își propune să pună față în față tinerii cu visele, întrebările și problemele lor și acei oameni care au expertiza și pot limpezi aceste aspecte legate de noua strategie de securitate, de implicațiile tot mai profunde ale mediului internațional cu cel intern, cu apariția intermesticului în această fază a globalizării, pe drumul integrării în UE, o piață liberă pentru persoane, capitaluri, tehnologii și informații. Venim cu inițiative ce crează punți în înțelegerea acestor probleme ce apar la suprapunerea a seturi diferite de cunoștințe, credințe, valori culturale, valori ce rămân totuși diferite, chiar și în această explozie informatică dominată de Internet .

Este un proiect ce implică parteneriatul public-privat, născut din inițiativa unor oameni cu preocupări în domeniul siguranței naționale ce au înțeles că spiritul civic se manifestă atât de puternic în coagularea interesului în structuri ce pot promova inițiative și asigura expertiza la 360 de grade a unei probleme și o agenție guvernamentală ce are ca scop sprijinirea inițiativelor tinerilor, a celor ce reprezintă viitorul, a celor ce mâine vor fi imaginea României.

ACTORII DE IMPLICAT

Agenția Națională pentru Sprijinirea Inițiativelor Tinerilor este un organism guvernamental ce gestionează în țara

noastră fonduri europene și guvernamentale românești destinate sprijinirii acțiunilor tinerilor, coagularea activității lor în nuclee civice, racordarea la valorile europene prin programe de schimb multinaționale, *traininguri* (inițiere, perfecționare, specializare), inițiative ce implică și tinerii proveniți din medii defavorizate sau cu dizabilități. Urmărește promovarea educației ne-formale și a acumulării de cunoștințe și norme de lucru în parteneriat cu persoane și organizații din alte țări europene, cu un alt background și o altă bază de cunoștințe și valori, cu o cultură și o bază de pregătire total diferită. În acest tip de programe constă și importanța activității agenției, ea reușește să creeze acel climat de lucru ce va caracteriza societatea românească după integrarea în Uniunea Europeană.

Asociația „Paideia" este o organizație ne-guvernamentală, formată din oameni politici, jurnaliști, militari și exponenți ai societății civile, toți absolvenți ai cursurilor Colegiului Superior de Siguranță Națională.

„Paideia" este persoană juridică română, de drept privat, fără scop patrimonial, ne-guvernamentală, apolitică, independentă de instituțiile publice de stat sau private, române sau străine. Asociația își propune să contribuie la promovarea și formarea culturii de securitate și la o mai bună articulare a mediilor politic, media, de informații și a societății civile în vederea promovării intereselor de securitate națională.

Principalele obiective ale Asociației sunt:

I. Constituirea unui Centru național de informare și documentare pe următoarele probleme: siguranță națională; educație; drepturile omului; politica externă a României pe linie de integrare euro-atlantică; relații academice.

II. Formarea în domeniul siguranței naționale (cursuri de specializare, tip școală de vară).

III. Formarea în domeniul securității (prelegeri, cursuri, seminarii, studii, proiecte). Tematica orientativă: organisme internaționale de securitate; societatea civilă și siguranța națională în diverse state; terorismul ca fenomen și combaterea lui; amenințări transfrontaliere; protecția mediului; siguranța națională și drepturile omului; politica de secu-

ritate a României; legislație; istoria serviciilor de informații și securitate.

IV. Editarea și difuzarea unor cărți și publicații periodice și ocazionale și a altor materiale de informare relevante pentru domeniul de activitate

V. Sprijinirea de studii științifice în aria de preocupare

VI. Cooperare cu organizații similare din țară și străinătate

Președintele Asociatiei „Paideia" este dl. Victor Adrian Vevera, absolvent al Colegiului Superior de Siguranță Națională, seria 2003. Asociația are drept scop principal promovarea educației pentru siguranța națională și are expertiza necesară pentru a demara un proiect în această arie.

Serviciul Roman de Informații în calitatea sa de principală instituție cu atribuții interne pe linia siguranței naționale este chemat să contribuie la edificarea unei solide culturi de securitate a cetățenilor propriei țări. De altfel, Serviciul a inițiat o serie de alte activități în această arie, între care amintim organizarea cursurilor Colegiului Superior de Siguranță Națională, publicarea de informații despre activitatea Serviciului pe pagina de Internet a instituției, editarea revistei de specialitate, „Profil", o strânsă colaborare cu mass-media.

Serviciul de Informații Externe instituție cu atribuții externe în ceea ce privește siguranța națională și promovarea intereselor României. În această arie este direct interesat de edificarea culturii de securitate a cetățenilor României. Cooperează cu Facultatea de Sociologie și Asistență Socială din cadrul Universității București, mai exact cu masterul de Studii de Securitate al Facultății, unde a furnizat specialiștii necesari pentru susținerea unui curs de un semestru pe tema „Democrația și securitatea națională".

Consiliul Suprem de Aparare a Țării coordonează activitățile de prezervare a securității naționale. A furnizat lectori și experiză necesară pentru instituțiile de învățământ superior care au desfășurat activitate didactică pe linia educației pentru securitate.

Academia Națională de Informații este o instituție militară de învățământ superior, creată în temeiul Legii privind

organizarea și funcționarea Serviciului Român de Informații, care prevede pregătirea personalului în cadrul unui sistem de învățământ propriu. În cadrul ANI, învățământul se desfășoară la standarde înalte de performanță, în acord cu Declarația Universală a Drepturilor Omului, Constituția României, Legea Învățământului, Legea privind acreditarea instituțiilor de învățământ superior și recunoașterea diplomelor, Statutul personalului didactic și Statutul cadrelor militare. Academia Națională de Informații are ca obiectiv principal formarea ofițerilor de informații, atât pentru Serviciul Român de Informatii, cât și pentru celelalte instituții cu atribuții în domeniul siguranței naționale. La încheierea studiilor, absolventii ANI obțin diploma de licență și brevet de ofițer. Instituția s-a implicat recent și în proiecte de promovare a culturii de securitate, cum ar fi organizarea cursurilor Colegiului Superior de Siguranță Națională, atât cu lectori din interiorul ANI, cât și cu personalități din afară. Academia dispune de o bază materială ce include sala de conferințe, mai multe săli de curs, bibliotecă, laborator de informatică, laborator de limbi străine, sală de sport, cabinet medical.

Colegiul Superior de Siguranță Națională a fost organizat după modelul *Citizen's Academy*, inițiat de *Federal Bureau of Investigations* (FBI). SRI a lansat în anul 2002 Colegiul Superior de Siguranta Natională, conceput ca o forma de deschidere a Serviciului Român de Informații către reprezentanți ai societății civile, personalități mass-media, lideri formali și formatori de opinie. Colegiul își propune în principal să ofere perspective noi în înțelegerea mizelor globale actuale. O modalitate în plus de a aprofunda, în parteneriat cu societatea civilă, o serie de concepte care devin din ce în ce mai actuale: criminalitate cibernetică, transfrontalieră, război neconvențional, amenințări asimetrice, terorism. O expunere la argumente din perspectiva *intelligence*-ului. Anul 2002 a însemnat racordarea Academiei Naționale de Informații, prin intermediul Colegiului Superior de Siguranță Națională, la circuitul valorilor de interes național, la transparență și deschidere spre societate.

Colegiul își propune obiective precise, cu rigurozitatea necesară înțelegerii rolului comunității informative și al societății în managementul activității de siguranță națională și nu al unei singure instituții de profil, în special Serviciul Român de Informații: cunoașterea principalelor instituții cu atribuții în domeniul securității și apărării naționale; formarea unei viziuni unitare asupra principalelor elemente care definesc securitatea națională și internațională; fundamentarea necesității integrării României în organismele de securitate europene și euroatlantice; înțelegerea dimensiunilor și riscurilor la adresa securității naționale la început de mileniu; cunoașterea modurilor de participare a societății civile la realizarea securității naționale; cunoasterea principalelor organizatii europene si nord-atlantice cu atributii în domeniul securității; cunoașterea matricilor de securitate ale României.

Proiectul modulelor gestionate de Asociaţia Absolvenţilor Colegiului Superior de Siguranţă Naţională „PAIDEIA" în cadrul Universităţii de vară organizată de ANSIT „Educaţia pentru Securitatea Naţională"

Durata cursurilor: 7–10 zile Module de studiu:

I. Fundamentele securității naționale: instituții; legislatie; context istoric; abordare psihosociologică; elemente de educație contrainformativă;

II. *Statul și securitatea națională*: reforma instuțională — necesitate, obiective; reforma legislativă — necesitate, obiective, context economic și securitate națională; percepția cu privire la securitatea națională — seminar.

III. *Securitate națională și securitate colectivă*: opțiunile NATO, UE și ONU privind securitatea colectivă; riscuri și amenințări asimetrice, atipice, nemilitare, neconvenționale; coordonatele de securitete — pacea caldă de după războiul rece; perspective — discuții libere.

IV. Relații internaționale și securitate națională: prezentarea principalelor teorii; zone de conflict — istoric, actori, evoluții, perspective; nevoia de informații în relațiile inter-

naționale; informații secrete și relații deschise; enlargement, integrare, globalizare — un nou context al securității — prelegere, discuții.

Obiective:

Construirea unei perceptii realiste despre sistemul de securitate națională; conștientizarea cu privire la necesitatea echilibrului dintre cerințele societății democratice și necesitatea de a prezerva securitatea națională; deschiderea apetitului spre acest domeniu.

Finalizarea se va putea realiza prin prezentarea unei lucrări pe o temă legată de securitatea națională în cadrul seminarului: „Securitatea națională și democrația".

Iată, așadar, câteva dintre gândurile și proiectele recente ce vizează educația pentru cunoașterea problematicii de securitate națională, ce reprezintă nu numai un obiectiv înscris în actuala Strategie de Securitate Națională a României, ci un interes social reclamat de evoluția firească a tinerei democrații românești spre un mediu de integrare euro-atlantică. În esență, pledăm pentru ca tinerii României să beneficieze nu numai de educația fizică, educația culturală, educația sanitară, educația civică, educația rutieră, educația religioasă ori a bunelor maniere, etc., ci și de o educație de securitate.

SECURITATEA NAȚIONALĂ — O ABORDARE COMPREHENSIVĂ

Vasile Eftimie

Evoluția actuală a omenirii, relațiile interumane, sociale și interstatale determină o diversificare a nevoilor de cunoaștere și de informare. Practic nu există domeniu de activitate, proces decizional în care să nu fie nevoie de o documentare informațională din ce în ce mai amplă, mai diversificată.

Schimbările rapide în situația politico-militară internațională continuă să surprindă serviciile de informații și analiștii ce nu aparțin serviciilor speciale. Importanța pe care a căpătat-o *informația*, amploarea procesului de cunoaștere a determinat constituirea unor organe specializate, la diferite nivele și domenii de activitate pentru culegerea de informații. La nivelul structurilor centrale ale statelor, precum și la nivelul structurilor specifice diferitelor domenii de activitate: politice, economice, tehnico-științifice, militare, etc., au fost constituite organe de informații specializate pe domeniile de interes. Marea majoritate a serviciilor de informații sunt subordonate la nivel central, sunt militarizate și considerate elemente ale sistemului național de apărare.

Sunt emise păreri conform cărora serviciile de informații ar trebui să acționeze pentru a previziona și apoi a monitoriza majoritatea fenomenelor, dacă nu totalitatea acestora. Realitatea confirmă o oarecare ineficiență în previzionarea evoluției fenomenelor politico-militare internaționale complexe, îndeosebi a conflictelor militare, fapt ce generează neîncredere și chiar acuze din partea conducerilor politico-militare și opiniei publice din anumite state.

Ceea ce se cunoște și se publică despre conflictele militare, rolul serviciilor de informații care au executat cercetarea strategică în cadrul acestor conflicte este foarte arid, de multe ori datele reale privind planificarea, desfășurarea și rezultatele acțiunilor militare fiind inaccesibile celor interesați. Istoricii și analiștii militari se rezumă, în cele mai multe

situații la descrierea clasică: cauzele, forțele implicate, desfășurarea, consecințele și învățămintele rezultate. Dar, apare și întrebarea: câți dintre comandanții militari participanți la un conflict și apoi istoricii și analiștii militari cunosc cauzele reale ale conflictului? Și în prezent se desfășoară cercetări privind cauzele reale ale celui de-l doilea război mondial, ale Războiului din Golf, din spațiul ex-iugoslav, etc. După un conflict militar sunt publicate date statistice privind folosirea unor categorii de forțe armate, genuri de arme și asigurarea logistică. În schimb, datele și informațiile privind modul cum s-a executat cercetarea sunt limitate, de multe ori inexacte, sau chiar lipsesc. Odată cu deschiderea arhivelor se descoperă din documente oficiale, aspecte reale privind rolul cercetării într-un anumit conflict militar. Sunt și unele situații când partea învingătoare dezvăluie modul cum adversarul a conceput și executat cercetarea.

Menținera și apariția unor centre de conflict, divergențele de ordin etnico-religios, tendința de revizuire a frontierelor actuale, instabilitatea economică și în general amenințările ne-militare la adresa multor state, determină ca serviciile de informații să-și amplifice activitatea, să-și mențină efective suficiente numeric și bine pregătite, iar fondurile alocate pentru funcționarea acestor servicii să crească de la an la an.

Schimbările produse în spațiul ex-sovietic și în Europa de Est, reducerile de efective militare, orientarea politicii externe a statelor din zonele amintite funcție de noile situații au determinat adoptarea de măsuri concrete pentru redimensionarea, reorganizarea și reorientarea activităților serviciilor de informații. Sunt valabile și astăzi cele afirmate de Wilhelm I în urma unei victorii a armatei prusace asupra francezilor: în timp ce adversarul a avut o sută de bucătari și un spion, noi am avut un singur bucătar și o sută de spioni!

De-a lungul timpului serviciile de informații au servit pe cei ce le-au constituit, subvenționat și folosit, culegând informații atât despre adversari, cât și despre prieteni. Și astăzi serviciile de informații, indiferent ce denumire poartă, urmăresc același scop: să asigure informații precise și la timp pentru factorii decizionali.

EVOLUȚIA CONCEPTULUI DE SECURITATE

Până în anii 1980, conceptul de securitate avea un rol subsidiar în analizele geopolitice, fiind dezvoltat cu precădere în domeniul militar, în cadrul studiilor strategice. În domeniul relațiilor internaționale, nu exista o școală de gândire coerentă care să dezvolte acest concept, el fiind relaționat cu principalele concepte care sunt dezvoltate în școlile relațiilor internaționale. Astfel, se pot distinge două abordări care au dominat gândirea referitoare la problema securității naționale, până în anii '80:

- **„securitatea ca un derivat al puterii"**
- **„securitatea o consecință a păcii"**

La începutul anilor '50, John Hetrz, elaborează conceptul de **„dilemă a securității"**, larg folosit în literatura de specialitate, care este „o noțiune de structură în care încercările de ajutorare ale statelor de a-și asigura propriile nevoi de securitate, tind, indiferent de intenție, să ducă la o creștere a insecurității celorlalți, întrucât fiecare interpretează propriile-i măsuri defensive, iar pe cele ale celorlalți ca fiind potențial amenințătoare[154].

Această abordare nu reușește să se impună în cercetările din mediul Războiului Rece, care erau centrate pe dinamica acțiune-reacțiune între puterile rivale.

În anii '70, Robert Jervis, prin lucrările sale, îndrepta atenția către elementele neintenționale și de interdependență dintre relațiile de securitate, lansând ideea de „regimuri de securitate", și introduce în cercetare nivelul de analiză sistemic.

Lipsa unei dezvoltări conceptuale pentru noțiunea de „securitate" poate fi privită, din punctul de vedere al lui Barry Buzan[155], din cinci perspective:

1. conceptul este prea ambiguu și complex pentru a-i atrage pe analiști; este „un concept esențialmente contestat".

---

[154] Barry Buzan, *Popoarele, statele și teama*, Editura cartier, 2000, p. 16.

[155] *Ibidem*, p. 19–23.

2. suprapunerea conceptului de putere peste cel de securitate. Securitatea devenea rezultatul concentrării puterii în mâinile unui stat sau grup de state ori consecință a menținerii balanței de putere. Critica ce este adusă este că „puterea poate deveni esența securității în situații de confruntare intensă sau de conflict, dar a considera că această identificare este valabilă întotdeauna creează riscul unei profeții condamnate să se împlinească"[156].

3. revoltele împotriva ortodoxismului realist de până la sfârșitul anilor '70. Școala Realistă făcea față acuzațiilor venite din partea Școlii Idealiste[157] și în același timp opunea conceptul de „putere" celui de „interdependență", venit din domeniul analizelor economice. La aceasta se adaugă diversificarea metodologică din anii '50–'70 care a cuprins domeniul relațiilor internaționale.

4. subdezvoltarea studiilor strategice.

5. ambigiutatea simbolică menținută de politicienii de stat, „o noțiune nedefinită de securitate națională oferă elitelor politice și militare o sferă de acțiune pentru maximizarea strategiilor puterii"[158].

În 1988, M. Allagappa, prin lucrarea „Comprehensive Security: Interpretation in Asean Contries"[159], chema comunitatea științifică la o abordare „comprehensivă" și „totală" a conceptului de securitate națională în conformitate cu totalitatea și multidimensionalitatea amenințărilor. Tot în 1988, Barry Buzan introduce conceptul de „complex de securitate"[160] în analiza pe care o realizează asupra dimensiunilor secu-

——— [156] *Ibidem.*

——— [157] Idealiștii respingeau modelul realist ca fiind periculos de autosatisfăcător și mult prea îngăduitor cu o lume a înarmării nucleare.

——— [158] Barry Buzan, *op.cit.*, p. 29–23.

——— [159] În lucrarea coordonată de Scalapino R., *Asian Security Issues: Regional and Global*, Berkeley, Institute for East Asian Studies, 1988.

——— [160] „Un complex de securitate se definește ca un grup de state ale cărui prime preocupări de securitate le leagă laolaltă suficient de îndeaproape, întrucât securitățile lor naționale să nu poată fi luate în considerare în mod realist separat una de alta (...) Complexele de securitate subliniază interdependența rivalității, precum și pe cea a intereselor împărtășite", Barry Buzan, *op.cit.*, p. 196.

rității în sud-estul Asiei și îl dezvoltă în lucrarea „People, States and Fear: An Agenda for International Studies in the Post-Cold War Era", apărută în 1991. De asemenea, subliniază necesitatea stabilirii unor nivele de analiză: „Intrucât realitatea interdependenței securității este inevitabilă, singura speranță pentru definirea unor subiecte de studiu manevrabile, care nici să nu se piardă, dar nici să nu sucombe în fața sensului vital al întegrului, este găsirea unei ierarhii a nivelurilor analitice în sistemul internațional. Fiecare dintre aceste niveluri trebuie să identifice trăsături durabile, semnificative și în mod substanțial independente ale problemei securității"[161]. Conceptul de „complex de securitate" este construit la nivel regional pe dinamica pattern-ului amiciției („de la simpla prietenie la pretinderea de protecție și ajutor"[162]) și inamiciției („relații stabilite prin suspiciune și teamă"[163]). Barry Buzan reușește să îmbogățască conceptul de securitate din domeniu relațiilor internaționale și să treacă către o perspectivă holistică a neorealismului, înlăturând critica etnocentrismului[164].

Aceste două evoluții circumscriu principalele dualisme conceptuale ale securității în jurul cărora se dimensionează noțiunea, în anii '80:

- securitate-anarhie; securitatea este rezultatul, fie al menținerii balanței de putere (modelul bipolar sau pantapolar), fie al afirmării unui sistem internațional hegemonic (modelul unipolar).
- securitate-comunitate; comunitatea de interese creează structuri comunitare de securitate, respectând legile proximității.
- securitate-apărare[165].

---

[161] *Ibidem*, p. 193.

[162] *ibidem*, p. 196.

[163] I*bidem*.

[164] Vezi studiul realizat asupra complexului de securitate din Insulele Britanice de către Wright Joanne, *Northern Irleand, A British Isles Security Complex*, Terorism and Political Violence, vol. 5, nr. 4, 1993, p. 266–286.

Din punct de vedere structural, există două abordări ale dimensiunilor conceptului de securitate: din teoria structurală a lui Kenneth Waltz se păstrează nivelele la care aceasta acționează: individual, statal și internațional[166]; din teoriile interdependenței s-au păstrat domeniile în care conceptul de securitate acționează: militar, politic, economic, social și mediu.

De la începutul anilor '90, în literatura de specialitate a relațiilor internaționale, unde paradigma dominantă era realismul, se afirma o nouă paradigmă — cea a constructivismului. Realiștii care au abordat teorii structurale sau sistemice, inspirate din teoria politicilor internaționale a lui Kenneth Waltz, au fost principala țintă a școlii constructive care îi acuzau că pierd din analiză factorul determinant, și anume, impărtășirea intersubiectivă a ideilor, care generează comportamentul prin constituirea identităților și intereselor actorilor. Rezultatul efortului acestei școli este de a diversifica și îmbogăți literatura de specialitate cu numeroase modele de cum normele, cultura, identitatea, încrederea, persuasiunea, învățarea, efectele de demonstrație, fluxurile conceptuale transnaționale, socializarea și multe alte procese ideaționale influențează sfârșitul dramatic al rivalităților marilor puteri[167].

Postulatele constructivismului sunt:

• politicile globale sunt rezultatul împărtășirii intersubiective a ideilor, normelor și valorilor, la nivelul actorilor. Constructiviștii se centrează pe dimensiunea intersubiectivă a cunoștințelor, deoarece ei doresc să sublinieze aspectul social al existenței umane — rolul ideilor împărtășite în structura ideațională de constrângere și dirijare a comportamentului;

——— [165] Vezi capitolul 7 din lucrarea citată a lui Barry Buzan.

[166] Kenneth Waltz, *Man, the State an War: A Theoretical Analysis*, Columbia University Press, 1954, tradusă în limba română de Mihaela Sadovschi: Kenneth Waltz, *Omul, statul și războiul. O analiză teoretică*, Ed.Institutul European, Iași, 2001.

[167] Brooks Stephen, *Powr, Globalizations and the End of the Cold War*, International security, 200/2001, vol. 25, nr. 3.

• structura ideațională nu are doar un efect regulativ, ci unul constructiv, asupra actorilor;

• între structurile ideaționale și actori (agenți) există a dublă direcție: de determinare și de constituire. Structurile constituie actorii, în termenii intereselor și identității lor, iar structurile sunt, la rândul lor, produse, reproduse sau alterate de practicile discursive ale agenților[168].

Diversitatea de abordări a conceptului de securitate și coagularea unor școli de gândire în domeniul relațiilor internaționale, nu face decât să indice principale direcții de cercetare, care, combinate, permit o operaționalizare a securității.

SECURITATE COMPREHENSIVĂ. SECURITATEA INDIVIDULUI

Noțiunea se dezvoltă prin transformarea conceptului „dezvoltarea individului" (human development), noțiune larg folosită în anii '60 și '70[169]. Precum conceptul de „dezvoltare a individului" așa și cel de **s.i.** are în centru individul ca element al societății civile, atenția centrându-se nu pe stat, ci pe comunitatea din care face parte individul.

Deși nu este clar definit, două tipuri de factori îi circumscriu dimensiunea[170]:

• **Factori interni** — (în) existența unui sistem de valori, dezechilibre economice acute, degradarea standardelor de viață, scăderea accesibilității la sistemele de educație, creșterea ratei de șomaj, dezvoltarea pieței informale, alterarea mediului înconjurător și lipsa unor mijloace eficiente de a acționa, creșterea incapacității sociale și de sănătate de a răspunde noilor probleme;

---

[168] Copeland Dale, *The Constructivist Challenge to Structural Realism*, International Security, Vol.25, nr. 2, 2000.

[169] Viorica Zorita Pop, *Human Security in Transition Societes*, NATO Review, 2002, p. 10.

[170] Ibidem.

• **Factori externi** care amenință realizarea securității individuale — sistemul de securitate internațional, instabilitatea politică, tensiunile politice, sociale, economice, naționale și militare, creșterea criminalității internaționale și dezvoltarea traficului cu materiale radioactive.

De asemenea, circumscrie și șapte dimensiuni[171] **s.i.**:
– securitate economică:
– securitatea hranei;
– securitatea sănătății;
– securitatea mediului;
– securitate personală;
– securitatea comunității;
– securitatea politică.

Securitatea comprehensivă este rezultatul conceptului de securitate, înțeles în strânsă legătură cu amenințările la care răspunde. Lărgirea agendei de securitate, care devine mai comprehensivă, privește atât identificarea și înțelegerea amenințărilor, cât și necesitatea și modalitățile de răspuns. Principalele amenințări identificate sunt:

• *Amenințări politice*: instabilitatea politică internă, eșecul statului, terorism, abuzul drepturilor omului;

• *Amenințări economice*: sărăcie, creșterea diferenței dintre țările sărace și cele bogate, crizele financiare internaționale, impactul unor state puternice economic asupra țărilor instabile vecine și pirateria;

• *Amenințările mediului*: dezastrul nuclear, schimbările ecologice globale, degradarea pământului, apelor, lipsa hranei și a celorlalte resurse;

• *Amenințări sociale*: conflictele majoritate/minoritate, suprapopularea, crima organizată, traficul de droguri transfrontalier, comerțul ilegal, imigrația masivă necontrolată și epidemiile.

Un efect negativ al lărgirii agendei de securitate este ca serviciile de securitate oferite de organizațiile legitimate să folosească forța, să ordone uzul de forță și să folosească amenințarea cu uzul de forță pentru a apăra cetățenii și statul,

——— [171] Ibidem, p. 24–25.

pot deveni mult prea puternice dacă devin prea active în sectoarele nemilitare ale societății. Mai mult, există posibilitatea ca serviciile de securitate să nu aibă expertiza necesară pentru a răspunde noilor amenințări.

COMUNITATEA DE INFORMAȚII A ROMÂNIEI. TRADIȚIE ȘI MODERNITATE

dr. Lionede Ochea

SCURT ISTORIC AL STRUCTURILOR INFORMATIVE ROMÂNEȘTI

Prima structură informativă și contrainformativă creată în țara noastră a fost Ministerul de Interne, cu acest nume din 1861, care fiinţase anterior sub denumirile de: Vornicie, Departamentul Treburilor din Lăuntru, Ministerul Afacerilor Interne. În subordinea lui funcționau Poliția de Siguranță și Inspectoratul General al Jandarmeriei. Din 1892 apare Direcția Administrației Generale a Personalului și Poliției de Siguranță - Biroul Siguranței Generale, urmată, în 1903, de Serviciul Poliției Generale și Statistici și de Direcția Poliției și Siguranței Generale din 1908. Ca organe exterioare erau Brigăzile de Siguranță și Serviciile Speciale de Siguranță. În cadrul Prefecturii Poliției Capitalei exista un Serviciu de Siguranță și Brigăzi Speciale de Siguranță.

În timpul primului război mondial structurile informative se diversifică și funcționează în subordinea Marelui Stat Major - Secția II cu Biroul 5 Informații și a Marelui Cartier General - Biroul 5 Informații. În paralel funcționau Brigada Specială de Siguranță, Serviciul de Informații româno-rus - sub conducerea inspectorului de poliție Romulus Voinescu și a omologului său rus, generalul Leontovici și o structură care colabora cu specialiștii francezi din cadrul Misiunii Speciale condusă de Henri Berthelot.

În cadrul operațiunilor de dezinformare a Comandamentului Puterilor Centrale se va remarca *Echipa Specială de Siguranță a Deltei Dunării*, condusă de Mihail Moruzov. Trimis în martie 1917 la Ismail, Mihail Moruzov va colabora cu agenți ce cunoșteau limba lipovenilor, unii vorbind și bulgara și germana. Zona a fost împărțită în 3 sectoare - Sulina, Vâlcov, Ismail - în ultimul oraș având centrul și Serviciul de Informații al Armatei Ruse prin Alexandru Escholtz,

fost agent corupător, având sarcina de a provoca dezertarea cadrelor românești la ruși.

Din 1920 va funcționa Secția V Informații și Contrainformații, în cadrul Diviziei II a Marelui Stat Major, care coordona activitatea: Biroului 1 informații — prelucra și sintetiza sub formă de buletine, broșuri, note, datele referitoare la armatele europene; Biroului 2 contrainformații — culegea informații militare din exterior, contrainformații, contraspionaj, cenzură, propagandă. Moruzov propune generalului Samsonovici, șeful Marelui Stat Major, o reorganizare a Serviciului Secret, după modelul Intelligence Service, a Serviciului Special de Informații, cu acoperirea punctelor cardinale sub denumirea de Frontul de Est, Sud și Vest. Schema de organizare a Serviciului Secret va fi aprobată abia în 1934 și va rămâne aproape neschimbată până la începutul celui de-al doilea război mondial

Între 1924–1929 Direcția Poliției de Siguranță avea în subordine: Serviciul Siguranței, Serviciul Controlului Străinilor și 4 Brigăzi centrale. În teritoriu, atribuții de siguranță reveneau Brigăzilor de Siguranță din centrele urbane, Inspectoratelor Regionale de Poliție și Siguranță, Chesturilor de Poliție din reședințele de județ.

În 1930 a fost înființată Direcția Generală a Poliției, în subordinea căreia se afla, printre alte structuri, *Direcția Poliției de Siguranță de Stat*, care coordona activitatea Serviciului de Informații, cu patru birouri: Siguranță Socială și a Informațiilor, Secretariat și Cifru, Studii, Presă, Buletinul Populației, Evidența statistică, arhiva și registratura, Serviciului de Control al străinilor. Alături de aceasta, cu atribuții informative mai ființa *Corpul Detectivilor* — supraveghere, filaj, interceptări telefonice și corespondență.

Serviciul Poliției de Siguranță (din 1942), cu atribuții informative, represive și preventive cu următoarele structuri specializate: Biroul de Informații - mișcarea fostelor partide politice, mișcarea comunistă, iredentele, francmasoneria, sectele interzise, străini, refugiați politici, dezertori, agitații politice, profesionale și economice; Biroul de Contrainformații - persoane suspecte de spionaj, terorism, sabotaj, defetism,

alarmism, anti-militarism, instigări la greve; Secretariat și redacția Buletinului Informativ; Evidență și statistică; Presă și translatori; Suspecți internabili în caz de mobilizare; Registratura, arhive, fișe; cinci birouri de siguranță, corespunzătoare chesturilor; 34 birouri de siguranță, corespunzătoare comisariatelor.

Alte instituții implicate în culegerea de date au fost cele subordonate *Ministerului Apărării Naționale.* După modelul francez al Secției Statistice este creată în cadrul Marelui Stat Major, Secțiunea II, în preajma primului război mondial fiind organizată în două diviziuni: Divizia I — studierea, analizarea și sintetizarea datelor referitoare la armatele puterilor europene și statelor balcanice; Divizia II - cu sarcini specifice contraspionajului militar, care coordona Serviciul interior — contraspionaj, Serviciul exterior - cu rezidenți interni și externi; Serviciul mobil - cu agenți de control și de legătură.

Pe teritoriul țării activitatea contrainformativă era condusă de Direcția Generală a Poliției și Inspectoratul General al Jandarmeriei. Exista și un organism contrainformativ mixt - Consiliul de Colaborare - la nivelul tuturor județelor, formate din prefect, șeful poliției, reprezentanții parchetului și ai garnizoanei, șeful legiunii de jandarmi, comandantul companiei de grăniceri.

La sfârșitul anului 1946 activitatea contrainformativă va dobândi tot mai mult un caracter politic, un rol deosebit avându-l reprezentanții sovietici din Comisia Aliată de Control. Apar astfel noi compartimente: Biroul Siguranță; Biroul Anchete și Control; Biroul Evidență - Fișier (cunoașterea cadrelor).

EVOLUȚIA SERVICIULUI SPECIAL DE INFORMAȚII

Serviciul Secret de Informații (SSI) a fost înființat după terminarea primului război mondial, când s-a pus problema reorganizării unui serviciu de informații și contrainformații în cadrul Marelui Stat Major. Deși s-a ajuns la concluzia că noul serviciu secret, pentru a fi mai eficient, va funcționa în paralel - având angajați civili, după modelul serviciului civil

francez - într-o primă etapă SSI a funcționat în subordinea Marelui Stat Major. Abia în 1922, Consiliul Superior al Apărării Țării i-a acordat mai multă autonomie, atât în plan informativ, față de Marele Stat Major, cât și în plan contrainformativ, față de Siguranța Generală. Serviciul Secret de Informații a fost reorganizat în 1923 și 1924, în 1925 fiind numit în fruntea sa Mihail Moruzov, personaj aproape legendar, sub a cărui comandă SSI a devenit principala instituție de profil a țării. Contribuția lui Moruzov la organizarea, reorganizarea și funcționarea timp de 15 ani a Serviciului Secret de Informații al Armatei Române, ne îndreptățește să îl considerăm creator exclusiv al acestei instituții.

SSI era compus din două secții: secția de informații și secția de contrainformații. În 1928, Moruzov a elaborat un proiect ambițios de reorganizare a SSI și a tuturor celorlalte servicii de informații, urmărind ca prin concentrarea tuturor sub o singură direcție generală să le aducă la nivelul serviciilor echivalente din SUA, Franța și Anglia. Deja în 1928, structura SSI se mărise considerabil, compunându-se dintr-un secretariat general și mai multe secții, cu o organizare importantă în întreaga țară. SSI continua să funcționeze sub tutela Marelui Stat Major, dispunând însă de autonomie - atât în ceea ce privește structura cât și organizarea — față de serviciul de informații al armatei. **La 11 ianuarie 1929, Marele Stat Major a prezentat Ministerului Apărării Naționale referatul nr. 171 cu propunerea de înființare a Serviciului Secret**, organ pentru culegerea de informații militare de sine stătător. Referatul este aprobat, iar **Mihail Moruzov a fost însărcinat cu organizarea acestui serviciu**, subordonat direct Marelui Stat Major.

Între anii 1929 — 1934, Serviciul Secret de Informații nu a avut, totuși, o organizare prea bine conturată, îi lipseau cadrele calificate și mijloacele tehnico-materiale și financiare necesare. În această perioadă, comunitatea informativă românească era formată din Serviciul Secret, Corpul Detectivilor din Siguranță, Secția a II-a din Marele Stat Major,

Structura informativă a Jandarmeriei și Serviciul Special de Informații al C.F.R.

În anul 1934, ca urmare a venirii la putere a lui Hitler în Germania, Serviciul Secret de Informații a fost reorganizat și întărit, pentru a face față noilor sarcini pe care urma să le îndeplinească în țară și pe plan extern. **La 20 aprilie 1934 s-a elaborat Regulamentul Serviciului Secret**, care prevedea scoaterea acestui organ din subordinea Marelui Stat Major (Biroul 2) și trecerea lui în cadrul Ministerului Apărării Naționale — Secretariatul General, lărgirea competențelor sale — acordându-i-se în același timp o independență sporită — reorganizarea pe principii bine conturate și dotarea cu mijloace materiale și financiare suficiente. Pentru prima dată, în schema organizatorică a Serviciului Secret figurează, în mod distinct, Secția de informații externe (Secția I-a), alături de Secția a II-a — de contrainformații, informații interne și de Secretariat.

Unul dintre elementele de noutate aduse de reorganizare a fost faptul că între cadrele SSI intrau și militari, detașați din armată. Un alt element de noutate l-a constituit înființarea, începând cu 1 octombrie 1936, a postului de consilier juridic, ocupantul acestuia lucrând direct cu șeful serviciului și fiind însărcinat cu „examinarea mersului urmăririlor și culegerea probelor, cu avizarea asupra oportunității juridice de declanșare a operațiilor, îngrijindu-se să nu fie prematur sau tardiv efectuate, în raport cu probele necesare în justiție".

Perioada octombrie 1939 – mai 1945 a reprezentat pentru comunitatea informativă a României — în care rolul de coordonare, analiză și sinteză i-a revenit Serviciului Special de Informații — o etapă importantă, caracterizată prin numeroase reorganizări cu efect direct asupra volumului activității desfășurate, asupra locului și rolului pe care l-a jucat în viața statului și în economia războiului.

În perioada premergătoare și imediat după izbucnirea celui de-al doilea război mondial, teritoriul românesc a devenit zonă de maximă importanță pentru interesele germane, franco-engleze și sovietice, duel soldat cu serioase prejudicii

pentru poporul nostru. Obiectivul strategic fiind, pentru români, refacerea tuturor granițelor țării, s-a declanșat o laborioasă activitate de creare și reformare a acelor instituții care puteau fi de folos în acest scop.

La 9 octombrie 1939 s-a publicat în Monitorul Oficial Decretul–lege pentru organizarea și funcționarea Ministerului Apărării Naționale, în care, pentru prima dată, apărea titulatura de Serviciu Special de Informații, nefolosită în timpul lui Moruzov, impunându-se abia după preluarea de către Eugen Cristescu a conducerii sale. Decretul prevedea că Serviciul Special de Informații va fi subordonat direct Ministerului Apărării Naționale, Șeful Serviciului va avea gradul de director general, iar personalul nu va face parte din corpul funcționarilor publici.

După arestarea lui Mihail Moruzov, la 5 septembrie 1940, funcția de șef al Serviciului Secret de Informații al Armatei Române a fost deținută pentru scurt timp de către colonelul Ioan Nicolaid și apoi de către colonelul Ghiță Ștefănescu, ambii înlocuiți din funcție de Ion Antonescu. Serviciul de Informații era subordonat direct Conducerii Statului Român, iar ca prevederi bugetare și administrative, Secretariatului general al Ministerului Apărării Naționale. La conducerea Serviciului — care își schimbă denumirea în Serviciul Special de Informații — a fost numit în funcția de Director General Eugen Cristescu.

Prin cele trei reorganizări care au urmat, în noiembrie 1940, ianuarie 1942 și aprilie 1943, SSI a suferit profunde transformări structurale, de efectiv dar și de concepție, fapt ce ne îndreptățește să afirmăm că inițiatorul și realizatorul lor, Eugen Cristescu, poate să fie considerat de către istoria serviciilor secrete românești drept un adevărat reformator, demn continuator al operei începute de predecesorul său, Mihail Moruzov. Opera de reconstrucție a Serviciului a fost inițiată și derulată în condițiile unei puternice presiuni a evenimentelor politice interne și internaționale. În timpul lui Cristescu, SSI a fost conceput și reorganizat ca un serviciu

de informare generală, sub ordinele și directivele Conducătorului Statului, Mareșalul Ion Antonescu.

COLABORAREA SERVICIULUI SPECIAL DE INFORMAȚII ȘI CELELALTE INSTITUȚII ALE COMUNITĂȚII INFORMATIVE NAȚIONALE

Ca important mijloc de obținere și mai ales de verificare a informațiilor, dar care reprezintă în același timp și o situație de normalitate între serviciile și structurile specializate ale statului, ori între acestea și alte instituții similare din alte țări — pe probleme de interes comun — cooperarea și schimbul de informații are vechi tradiții, atestate documentar, în istoria serviciilor secrete românești.

Serviciul Special de Informații a colaborat cu toate serviciile, structurile specializate și alte instituții românești, ceea ce a reprezentat un aspect de modernitate, cu luminile și umbrele lui, specifice de altfel spațiului românesc.

La *Palatul Regal* informațiile ajungeau prin intermediul lui Ernest Urdăreanu, iar serviciile oferite erau permanente: Moruzov îl însoțește pe Carol II în vizita din Occident, beneficiind de surse suplimentare de finanțare a activităților informative. Mai mult, datorită acestui «ajutor», Înalta Curte de Conturi nu a exercitat nici un fel de control financiar asupra fondului pentru informații. Va avea un rol important în revenirea la putere a lui Carol II, prin favorizarea numeroaselor disidențe care au dus la fărâmițarea partidelor politice interbelice.

Convingerile antisovietice l-au făcut pe Moruzov să pună la dispoziția Parlamentului date care dovedeau implicarea sovieticilor în greva din februarie 1933, având și un rol important în desființarea societății *Amicii URSS*; cu toate acestea, asigura permanenta protecție a lui Nicolae Titulescu împotriva tentativelor de asasinat ale legionarilor, deși nu era de acord cu politica de înțelegere față de URSS dusă de acesta în anii '30. Datorită lui este anulat proiectul vânzării de avioane vechi românești către Mexic, pentru că astfel ar

fi implicat România în războiul civil din Spania, prin dotarea forțelor republicane. Cu această ocazie este trimis în Spania, cu aprobarea regelui, un «corespondent de război», devenit ulterior diplomat de carieră. Ca o dovadă de relații cel puțin cordiale, este semnificativ a aminti înscrierea personalului civil al Serviciului Secret în Frontul Renașterii Naționale în 1938; ulterior vor fi preferate cadrele care erau membre P.C.R. sau UTC.

De la Marele Stat Major și Ministerul Apărării Naționale, Mihail Moruzov a beneficiat de sprijinul și încrederea unor ofițeri. Mai întâi, maiorul Ioan Țăranu, șeful Biroului II contrainformații a Secției IV și colonelul Condeescu, în mai 1918, când Moruzov a fost acuzat de relații suspecte cu serviciile secrete bulgare și germane, ori cu membri ai comitetelor bolșevice sau că și-a dezinformat permanent superiorii și că a încurajat propaganda revoluționară, cei doi ofițeri de stat major au depus mărturii favorabile.

Structura informativă creată de Moruzov în primul război mondial și pusă sub autoritatea Marelui Cartier General al Armatei Române, va fi desființată în 1920. În 1925, cu sprijinul generalului Arthur Văitoianu, va fi reactivată. În privința calității informațiilor, șeful Secției II, generalul Simion Florescu afirma că acestea erau net superioare celor ale Siguranței Generale, când Marele Stat Major nu dispunea de un serviciu propriu de informații.

Din anii '30 va exista o stare de tensiune între Ion Antonescu, ca șef al Marelui Stat Major și Moruzov, dar, pentru a calma spiritele, Carol II muta Serviciul Secret din subordinea Marelui Stat Major la Ministerul Apărării Naționale (1934) și invers (1938). Până în august 1940 a fost omul de încredere al lui Carol II, dar imediat ce a fost bănuit că s-ar fi aliat cu legionarii, a fost îndepărtat. Din exterior primea de la unii atașați militari copii ale buletinelor informative lunare, pe care aceștia le trimiteau Secției II a Marelui Stat Major, dar nu toți au acceptat astfel de colaborare. Din 1940 este în subordinea Președinției Consiliului de Miniștri, iar din lipsă de fonduri suficiente va mai primi 1,5 milioane

lei pentru activități informative, din bugetul Marelui Stat Major.

Sintezele săptămânale erau structurate pe fronturi : Frontul de Est — URSS, Finlanda, Suedia, Japonia, China; Frontul de Vest — Ungaria, Germania, Franța, Anglia, Norvegia, Danemarca, SUA, Țările de Jos, Elveția, Slovacia, Belgia; Frontul de Sud - Bulgaria, Iugoslavia, Turcia, Iran, Irak, Grecia, Italia, Spania, Portugalia, Egipt.

Pentru delimitarea atribuțiilor Serviciului Secret de cele ale Marelui Stat Major sunt redactate *Instrucțiuni referitoare la delimitarea atribuțiilor și conlucrarea informativă a Marelui Stat Major și Serviciul Secret.* Primul avea ca responsabilități culegerea de informații de ordin militar de-a lungul frontierelor, cu competențe exclusive în armată, asigura legătura cu organele oficiale străine și studia și interpreta informațiile. Serviciul Secret culegea informații politice și militare în interiorul statului, cu competențe de contraspionaj, recrutare și pregătire de agenți informatori și confecționare a documentelor de identitate. Stabilea legătura cu serviciile de informații străine.

În februarie 1941 se face o altă delimitare a atribuțiilor, dar la nivel de ministere: Marele Stat Major - informații militare; Ministerul de Externe - informații politice și cele legate de minoritățile românești; Serviciul Special de Informații - informații militare, economice, politice sociale referitoare la românii cu dublă cetățenie. Se propunea dublarea personalului Consulatelor cu cadre militare specializate, sub acoperirea de atașați de presă, iar personalul diplomatic să fie pregătit informativ la sediul SSI. După 1944 își va rezuma activitatea la informații interne, simple verificări ale unor ofițeri și semnalarea unor elemente ostile regimului.

Sunt atestări documentare privind relațiile SSI cu *Siguranța Generală.* În timpul primului război mondial se înregistrează tensiuni între Moruzov și delegatul Siguranței Generale pe lângă armatele ruse din Basarabia, Romulus Voinescu. Consecințele negative ale fricțiunilor dintre Moruzov și Voinescu au dus la deconspirări reciproce de agenți sau

slab ajutor profesional acordat în cazuri limită. Tensiunile între cei doi vor continua de-a lungul întregii perioade, fiind nevoie de medierea personală a regelui Ferdinand, dar antipatia reciprocă nu a fost niciodată soluționată.

SSI a avut relații foarte bune cu *Inspectoratul General al Jandarmeriei și cu Prefectura Poliției Capitalei.* Ministerul de Interne va fi penetrat de oamenii Serviciului Secret din 1937, de când Moruzov se afla la conducerea SSI și a Direcției Generale a Poliției, dar și prin numirea ca șef al Corpului Detectivilor din Siguranța Generală a lui Niky Ștefănescu, bun și vechi colaborator al lui Moruzov. La recomandarea sa, Direcția Generală a Poliției, Corpul de Jandarmi și Prefectura Poliției Capitalei sunt unificate în Direcțiunea Generală a Poliților și Siguranței Statului.

Cu *Președinția Consiliului de Miniștri*, SSI s-a aflat în raporturi de subordonare, după venirea lui Ion Antonescu la putere și desemnarea lui Eugen Cristescu în funcția de director general. Pentru sintetizarea și centralizarea materialelor informative, a fost creat în 1940 Serviciul de Centralizare a Informațiilor, pentru informarea Președinției Consiliului de Miniștri cu date culese de Serviciul Secret și Secția II a Marelui Stat Major. Din decembrie 1941, Eugen Cristescu avea voie să participe la ședințele pe probleme interne ale Consiliului de Miniștri. Atenția deosebită acordată Serviciului este dovedită de ordinea priorităților telefonice la nivelul Președinției, care așeza Serviciul condus de Eugen Cristescu înaintea Cabinetului Militar al mareșalului Ion Antonescu. În timpul celui de-al doilea război mondial va fi implicat, din ordinul lui Ion Antonescu, în relațiile cu Aliații pentru ieșirea României din război și supravegherii oamenilor politici democrați.

Cu Ministerul de Interne, relațiile au fost fie reci, fie tensionate din cauza infiltrării cu elemente legionare a Ministerului, accentuată de venirea lui Eugen Cristescu la conducerea SSI și implicarea acestuia în reprimarea rebeliunii. Schimbul de informații se făcea prin adrese și buletine informative, dar se urmărea și strângerea relațiilor dintre șefi prin «mese

camaraderești» oferite de Siguranța Generală, Prefectura Poliției sau Secția a II-a a SSI.

Cu Ministerul Afacerilor Externe, la vârf, relațiile au fost foarte bune, fiind impulsionate și de simpatia între Eugen Cristescu și Mihai Antonescu. Pe de altă parte, informațiile externe erau obținute prin intermediul secretarilor, atașaților militari, cancelarilor, consulilor, viceconsulilor sau atașaților de legație, care puteau acționa sub protecția pașaportului diplomatic.

În general însă, la nivelul de jos, al agenților și funcționarilor diplomatici, relațiile au fost de dispreț și răceală reciproce. Agenții SSI îi acuzau pe diplomați de lipsa de pregătire în privința accesului la documente secrete și slabe cunoștințe de tehnică militară, ceea ce a dus la organizarea de cercuri de muncă informativă pentru atașații Legațiilor de către specialiști ai SSI. O altă problemă a fost controlul fondurilor speciale de către șeful misiunii diplomatice, sugestie refuzată categoric de Eugen Cristescu.

NECESITATEA ORGANIZĂRII ȘI COORDONĂRII UNITARE A ACTIVITĂȚILOR CARE PRIVESC APĂRAREA ȚĂRII ȘI SIGURANȚA NAȚIONALĂ

Pe plan mondial, prima mențiune oficială a conceptului de comunitate de informații a fost în Legea securității Naționale — National Security Act of 1947, care fundamentat reorganizarea sistemului informativ al Statelor Unite. Ulterior, acesta a fost aplicat de mai multe state, care au recurs la organizarea și reunirea activităților informative după principiile unei comunități a serviciilor secrete, chiar dacă acest cadru conceptual nu era reglementat.

Evoluția problematicii comunităților informative, mai ales în ultimii 15 ani, odată cu căderea „cortinei de fier", precum și caracteristicile geopolitice actuale relevă existența unei tendințe de conturare și consacrare formală, la nivel global, a comunităților informative, precum și consolidarea continuă a mecanismelor de coordonare executivă unitară. În afara

mecanismelor de subordonare particulară a serviciilor și de exercitare a controlului civil asupra acestora, s-au creat structuri coordonatoare centrale, plasate sub autoritatea politică a unei instituții (președinție, executiv și/sau legislativ), abilitată atât să coordoneze unitar și constant activitatea diverselor structuri din domeniu, cât și să dirijeze unitar, conform orientărilor doctrinare ale statului respectiv, resursele, ponderea, atribuțiile și rolurile concrete ale fiecărui serviciu. Fără îndoială, de la caz la caz, în fiecare comunitate informativă există un serviciu pilot, acesta fiind statuat în funcție de prioritățile obiective ale activității de realizare a siguranței naționale a fiecărui stat în parte.

Toată această coagulare a activității diverselor servicii de informații în comunități informative este efectul unor necesități obiective, cum ar fi: eliminarea informărilor disparate prezentate la nivelul deciziei politice; evaluarea unitară a informațiilor, stabilirea și actualizarea obiectivelor repartizate fiecărui serviciu în parte; eficientizarea cooperării și schimbului de informații, atât în plan intern, cât și extern; repartizare judicioasă a fondurilor financiare disponibile. Nu este mai puțin adevărat că, o coordonare unică a activității informative rezidă și din necesitatea integrării activităților de informații cu cele politico-diplomatice, militare, economice etc.

În ceea ce privește țara noastră, după cum am prezentat anterior, există o tradiție în existența și funcționarea unei astfel de comunități de informații, anterioare celei din Statele Unite. Astfel, reforma structurală și conceptual teoretică din domeniul dreptului polițienesc derulată la începutul deceniului al treilea al secolului trecut a creat treptat comunitatea informativă a României, cu rol de apărare a intereselor de securitate național-statală. Aceasta era formată din Consiliul Suprem de Apărare a Țării, Biroul Permanent al Micii Înțelegeri, structurile specializate din Ministerul de Interne (Direcția Poliției și Siguranței Generale, Jandarmeria rurală și Serviciul de Informații al regionalei Autonome CEFG) și serviciile de informații ale Ministerului Apărării Naționale

(Secția a III-a din Marele Stat Major și Serviciul Secret al Armatei Române — devenit ulterior Serviciul Special de Informații).

NOILE OBIECTIVE ÎN DOMENIUL SECURITĂȚII NAȚIONALE

Adoptată relativ recent prin Hotărârea Guvernului României nr. 36 din 18 decembrie 2001, Strategia de securitate a României este cel mai important act normativ din domeniul informațiilor, reprezentând documentul de bază care fundamentează planificarea apărării la nivel național, constituind expresia politică de referință a atributelor fundamentale ale statului român.

Țintele principale ale acestei strategiei de securitate le reprezintă: garantarea democrației și a libertăților fundamentale, dezvoltarea economică și socială susținută și durabilă, aderarea la NATO și integrarea în Uniunea Europeană, toate în raport de realitățile din societatea românească și din lume, precum și de perspectivele previzibile pe termen scurt și mediu ale vieții interne și internaționale.

Sistemul securității naționale este definit ca ansamblul reglementărilor și instituțiilor statului roman, care au rolul de a realiza, proteja și afirma interesele fundamentale ale statului roman.

Strategia de securitate națională cuprinde, în ordine: definirea intereselor naționale de securitate; precizarea obiectivelor care conduc la protejarea și afirmarea acestor interese; evaluarea mediului internațional de securitate; identificarea factorilor de risc din mediul intern și internațional; direcțiile de acțiune și principalele mijloace pentru asigurarea securității naționale a României.

Sunt fixate următoarele obiective:

– păstrarea independenței, suveranității, unității și integrității teritoriale ale statului roman, în condițiile specifice aderări la NATO și integrării în Uniunea Europeană;

– garantarea ordinii constituționale, consolidarea statului de drept și a mecanismelor democratice de funcționare a societății românești prin;

– relansarea economiei naționale, combaterea sărăciei și a șomajului;

– perfecționarea mecanismelor economiei de piață și a disciplinei financiare;

– dezvoltarea societății civile și a clasei de mijloc;

– asigurarea stabilității sistemului financiar-bancar și a echilibrului social;

– modernizarea instituțiilor de apărare a ordinii publice și garantarea siguranței cetățeanului;

– optimizarea capacității de apărare națională, în conformitate cu standardele NATO;

– îmbunătățirea capacității de participare la acțiunile internaționale pentru combaterea terorismului și a crimei organizate;

– îmbunătățirea stării de sănătate a populației, protecția copilului, dezvoltarea instituțiilor de educație, cercetare și cultură;

– reforma administrației publice și dezvoltarea regională în corelație cu practicile și reglementările europene;

– armonizarea relațiilor interetnice și edificarea statului civic multicultural, având drept garanții ale securității participarea socială, integrarea interculturală și subsidiaritatea în actul de guvernare;

– acțiuni diplomatice și o politică externă dinamică și pragmatică, bazată pe respectarea tratatelor și acordurilor internaționale la care România este parte, a obiectivelor și principiilor Cartei ONU;

– diversificare și strângerea legăturilor cu românii care trăiesc în afara granițelor țării;

– participarea activă la acțiunile de cooperare internațională pentru combaterea terorismului și a crimei organizate transfrontaliere;

– dezvoltarea relațiilor de bună vecinătate și a unei conduite participative pe plan regional, pentru consolidarea stabilității și reglementarea crizelor;
– asigurarea securității ecologice;
– implicarea societății civile în realizarea obiectivelor strategiei de securitate.

CADRUL LEGISLATIV CU PRIVIRE LA ATRIBUȚIILE INSTITUȚIILOR SISTEMULUI NAȚIONAL DE APĂRARE

După revoluția din decembrie 1989, au fost create, treptat, diverse servicii de informații, diferit subordonate și fără o delimitare netă a competențelor fiecăruia.

Prima lege din domeniu a fost Legea nr. 14/1990 privind organizarea și funcționarea Serviciului Român de Informații, care a precedat practic legea privind siguranța națională. Prin acest act normativ, S.R.I. are atribuții în cunoașterea, prevenirea și contracararea amenințărilor interne la adresa siguranței naționale.

Ulterior, a fost adoptată Legea nr. 51/1991 privind siguranța națională a României, care reglementează și definește amenințările la adresa siguranței naționale, specifice perioadei și contextului politico-social din perioada respectivă. În această lege sunt menționate și structurile informative cu atribuții de culegere și valorificare a informațiilor care, într-o măsură mai mare sau mai mică, funcționau deja: Serviciul de Informații Externe, Serviciul de Protecție și Pază, Serviciul de Telecomunicații Speciale, precum și structuri specializate din cadrul unor ministere (U.M. 0215, devenită ulterior U.M. 0962, din cadrul Ministerului de Interne, Serviciul Independent de Protecție și Anticorupție, transformat recent în Direcția Generală de Protecție și Anticorupție în cadrul Ministerului Justiției, precum și structurile informative ale Ministerului Apărării Naționale).

Cu o întârziere destul de mare, celelalte structuri informative au beneficiat de un cadru legislativ de funcționare, care să autorizeze activitatea acestora.

Astfel, la 24 iulie 1996 a fost adoptată Legea nr. 92 privind organizarea și funcționarea Serviciului de Telecomunicații Speciale, definit ca „organul central de specialitate cu personalitate juridică, ce organizează, conduce, desfășoară, controlează și coordonează activitățile din domeniul telecomunicațiilor speciale pentru autoritățile publice și pentru alți utilizatori".

La 6 ianuarie 1998 a fost adoptată Legea nr. 1 privind organizarea și funcționarea Serviciului de Informații Externe, prin care acesta este definit „ca organul de stat specializat în domeniul informațiilor externe privind siguranța națională și apărarea României și a intereselor sale".

În același an, la 19 octombrie a fost adoptată Legea nr. 191 privind organizarea și funcționarea Serviciului de Protecție și Pază, prin care acesta este învestit cu „asigurarea pazei demnitarilor români, a demnitarilor străini pe timpul ședерii lor în România, a familiilor acestora, în limitele competențelor legale, precum și în asigurarea pazei sediilor de lucru, a reședințelor acestora, potrivit hotărârilor Consiliului Suprem de Apărare a Țării".

Legea nr. 40 din 16 ianuarie 2002, privind completarea Legii nr. 40 din 18 decembrie 1990 privind organizarea și funcționarea Ministerului de Interne, aduce clarificările ce se impuneau în privința activităților informative desfășurate de structura specializată a ministerului. Astfel, este abilitat să „organizeze și să desfășoare, prin structuri de informații specializate, activitate de obținere, prelucrare, verificare, stocare și valorificare a informațiilor în domeniul misiunilor, patrimoniului și personalului ministerului, apărarea secretului de stat și de serviciu în cadrul instituției, precum și prevenirea și descoperirea infracțiunilor, identificarea factorilor de risc și amenințărilor la adresa ordinii publice".

Legea nr. 14 din 26 ianuarie 2001, privind organizarea și funcționarea Ministerului Apărării Naționale, prevede la

articolul 4, și Direcția Generală de Informații a Apărării, definită la articolul 17 ca „structura specializată a Ministerului Apărării Naționale care răspunde de obținerea, prelucrarea, verificarea, stocarea și valorificarea informațiilor și datelor referitoare la factorii de risc și amenințare externi și interni, militari și nonmilitari care pot afecta siguranța națională, de elaborarea concepției privind realizarea securității informațiilor și activităților criptografice și de asigurarea informațiilor geografice necesare armatei".

O instituție relativ recent înființată este Oficiul Registrului Național al Informațiilor Secrete de Stat, în baza Legii nr. 153 din 7 noiembrie 2002. Aceasta este o instituție publică cu personalitate juridică cu autoritate la nivel național în domeniul securității informațiilor clasificate.

În contextul integrării țării noastre în structurile NATO, prin Hotărârea Guvernului României nr. 354 din 15 aprilie 2002, au fost înființate Agenția de Acreditare de Securitate, Agenția de Securitate pentru Informatică și Comunicații și Agenția pentru distribuirea materialului Criptografic, care au competențe specifice pe linia stocării/procesării informațiilor clasificate NATO în cadrul sistemelor de prelucrare automată a datelor, respectiv transmise prin rețelele de comunicații a datelor.

În cele din urmă, cu o întârzierea apreciabilă, a fost adoptată și Legea nr. 415 din 10 iulie 2002 privind organizarea și funcționarea Consiliului Suprem de Apărare a Țării, autoritatea administrativă autonomă învestită, potrivit Constituției, cu organizarea și coordonarea unitară a activităților care privesc apărarea țării și siguranța națională.

COMUNITATEA DE INFORMAȚII A ROMÂNIEI — NECESITATE OBIECTIVĂ

Pentru prevenirea și contracararea tuturor amenințărilor interne și externe la adresa siguranței naționale, structurile informative organizează și desfășoară activități specifice.

Fără îndoială că, în activitatea informativă sunt inerente unele suprapuneri tangențiale de competențe, precum și complementarități ale rezultatelor activităților, totul pe fondul respectării deplinei legalități. Eficiența serviciilor de informații este direct proporțională cu calitatea și oportunitatea informațiilor pe care le transmit.

În contextul actual, caracterizat de o dinamică accentuată a evoluției vieții social-politice și economice, atât pe plan intern, cât mai ales extern, organizarea serviciilor de informații și a structurilor departamentale din cadrul diferitelor instituții cu atribuții în domeniu, existența acestora în cadrul unei comunități organizate și instituționalizate de informații permite evitarea paralelismelor și a suprapunerii de competențe, precum și eliminarea concurenței între acestea.

Necesitatea unei comunități de informații rezidă și din necesitatea de a înlătura dificultățile factorilor de decizie de a cuprinde și evalua unitar informațiile puse la dispoziție de serviciile de informații asupra unui context operativ, dat fiind că uneori, interpretarea datelor poate fi diferită, raport cu punctele de vedere ale serviciilor de informații, ce raportează individual. Totodată, în anumite conjuncturi operaționale, când se prefigurează fapte, împrejurări sau fenomene de amploare, cu implicații majore asupra intereselor țării, combaterea acestora reclamă o eficientizare a colaborării între instituțiile abilitate în aceste domenii.

Existența comunității de informații ar consacra, pe de altă parte, existența legală definitivă a instituțiilor cu competențe în culegerea de informații, eliminând totodată paralelismul structural și funcțional, de natură a genera blocaje în schimbul de informații, în procesul de informare a factorilor decizionali ce poate genera chiar dezinformări, precum și în soluționarea unor probleme operative, de natură a conduce la deconspirări. În plus, aceste paralelisme grevează și bugetul de stat.

Modificările survenite în mediul strategic de securitate au condus la concluzia că Legea nr. 51/1991 privind siguranța națională nu mai este de natură a oferi un cadru legal

complet. Pe de o parte, trebuie definit mult mai clar conceptul de amenințare la adresa siguranței naționale, precum și cel de interes major al statului român care trebuie protejat de către serviciile de informații. Totodată, trebuie definite clar competențele fiecărui serviciu de informații în parte. În spațiul public intern, dezbaterile privind organizare și funcționarea serviciilor de informații conduc către atribuirea de competențe în activitatea de informații numai SRI și SIE, celelalte structuri departamentale urmând să aibă competențe limitate la asigurarea îndeplinirii atribuțiilor specifice autorităților publice din care fac parte (Ministerul Apărării Naționale, Ministerul de Interne, ministerul justiției, S.P.P. și STS). În prezent, la Parlamentul României au fost depuse 4 proiecte de lege privind siguranța națională, care, în esență, propun constituirea comunității de informații.

BIBLIOGRAFIE

Marian Ureche, Aurel Rogojan, *Servicii secrete străine*, vol. 1. Editura Paco, București, 1999;

Istoria militară a poporului român, vol. VI, Editura Militară, București, 1989;

N.D. Stănescu, *Întâmplări și oameni din Serviciul Secret*, Editura Enciclopedică, București, 2002;

Cristian Troncotă, *Mihail Moruzov și Serviciul Secret de Informații al Armatei Române*, Editura

Evenimentul Românesc, București, 1997;

Cristian Troncotă, *Eugen Cristescu — asul serviciilor secrete românești*, Roza Vânturilor, 1994;

Cristian Troncotă, *Istoria serviciilor secrete românești. De la Cuza la Ceaușescu*, 1999;

Decretul-lege nr.3083, publicat în „Monitorul Oficial" din 25 septembrie 1940;

Hotărârea Guvernului României nr. 36 din 18.12.2001 privind Strategia de securitate a României, publicată în „Monitorul Oficial" nr. 822 din 20.12.2001;

Legea nr. 92 din 24 iulie 1996, publicată în „Monitorul Oficial" nr. 169 din 30 iulie 1996;

Legea nr. 1 din 6 ianuarie 1998, publicată în „Monitorul Oficial" nr. 7 din 12 ianuarie 1998;
Legea nr. 191 din 19 octombrie 1998, publicată în „Monitorul Oficial" nr. 402 din 22 octombrie 1998;
Legea nr. 40 din 16 ianuarie 2002, publicată în „Monitorul Oficial" nr. 75 din 31 ianuarie 2002;
Legea nr. 14 din 26 ianuarie 2001, publicată în „Monitorul Oficial" nr. 65 din 7 februarie 2001;
Legea nr. 354 din 15 aprilie 2002, publicată în „Monitorul Oficial" nr. 315 din 13 mai 2002;
Legea nr. 415 din 27 iunie 2002, publicată în „Monitorul Oficial" nr. 494 din 10 iulie 2002.

O PROPUNERE DE EVALUARE ORGANIZAȚIONALĂ A ROMÂNIEI

Dorlin Mureșan

Studiul de față propune *evaluarea unei țări — a României — prin elemente ale analizei și diagnozei organizaționale,* interconectând domeniul securității naționale cu acela al dezvoltării sustenabile și având drept scop identificarea acelor elemente ce pot constitui factori de succes în mediul competițional în care evoluează țara noastră. Supunem atenției elementele unor instrumente de evaluare organizațională care pot fi adaptate și incluse în evaluarea unei țări. Evaluarea organizațională a țării, deși poate include câteva din componentele care intră în analiza riscului de țară, nu trebuie confundată cu „ratingul" unei țări, întrucât scopul analizei nu este acela de a acorda un scor, sau o notă, ci de a oferi o imagine de ansamblu, care să servească drept punct de pornire pentru îmbunătățirile viitoare. Sunt expuse argumentele care justifică perspectiva organizațională în evaluarea securității unei țări și prezentate elementele de bază din evaluarea unei organizații și posibilele lor corespondențe la dimensiunile unui stat. Cadrul de analiză propus se concentrează asupra unor elemente direct legate de implicarea factorului uman în dezvoltarea organizatorică.

DE CE ESTE UTILĂ ABORDAREA ORGANIZAȚIONALĂ ÎN EVALUAREA NAȚIONALĂ?

Evaluare organizațională a unei țări presupune transferul unor concepte dinspre mediul economic și cel al organizațiilor neguvernamentale înspre domeniul securității naționale. Acest transfer se justifică în cazul României prin cel puțin trei argumente.

În primul rând, acest transfer de concepte se integrează în tendința actuală de a prelua dintr-un domeniu diferit acele

elemente noi, de progres, care pot, în urma adaptării, să ofere un avantaj competitiv în propriul domeniu de activitate. Transferul de concepte dintre domeniul securității (chiar și militare) și cel economic a făcut deja istorie. După ce analiza de risc a fost preluată din sfera analizei militare în domeniul afacerilor, modele de managemement și gestiune au fost adaptate pentru a răspunde nevoii de analiză și control al riscurilor la adresa securității naționale. Concepte ca *„intelligence competitiv"*, *„deficit de securitate"* și *„strategie de imagine a unei țări"*, respectiv *„branding de țară"* au început să fie vehiculate tot mai mult și în România, în domeniul securității naționale. Punerea în discuție a securității naționale din perspectiva evaluării organizaționale se înscrie astfel într-un proces natural de transfer al elementelor de analiză dintr-un domeniu de vârf într-altul, din dorința de a spori competitivitatea proprie. În plus, există exemple de succes în diferite țări despre rezultatele unor asemenea abordări transdisciplinare. Unul dintre exemplele concludente este *„National Partnership for Reinventing Government"*, proiect de îmbunătățire a funcționării administrației americane, inițiat de vice-președintele Al Gore, în 1993, în a cărui echipă de lucru au fost incluși consultanți specialiști în problematica managementului schimbării și dezvoltării organizaționale.

În al doilea rând, Strategia de Securitate Națională a României prevede afirmarea, realizarea și protejarea unor interese naționale, printre care: „dezvoltarea economică și socială a țării în pas cu dezvoltarea contemporană. Reducerea susținută a marilor decalaje care despart România de țările dezvoltate europene", „realizarea condițiilor pentru integrarea României ca membru NATO și UE" și „afirmarea identității naționale și promovarea acesteia ca parte a comunității de valori democratice; valorificarea și dezvoltarea patrimoniului cultural național și a capacității de creație a poporului român."

Dincolo de un exercițiu intelectual, transferul de concepte este necesar, pentru că România evoluează într-un mediu

tot mai competitiv. Schimbarea gradului de competitivitate a mediului se datorează în principal următorilor factori: pe de o parte este tendința generală spre o competitivitate sporită, aceasta fiind o caracteristică de bază a globalizării, iar pe de altă parte este traiectoria României de aderare la Uniunea Europeană.

Aici ținem cont de faptul că Uniunea Europeana intenționează să devină ea însăși tot mai competitivă pe plan mondial, după cum reiese și din Strategia adoptată în martie 2000 la Lisabona, prin care UE își propunea să devină cea mai competitivă economie din lume până în anul 2010. Chiar dacă la nivelul Uniunii Strategia Lisabona este departe de a obține rezultatele așteptate, ea exprimă o aspirație și tendință spre eficientizare. Este de așteptat ca această tendință să se transmită și la nivelul statelor membre. Competitivitatea în spațiul UE nu se referă doar la domeniul economic, ci se va face simțită tot mai mult și la nivel instituțional. Astfel România trebuie să dezvolte capabilitățile instituțiilor sale de a răspunde corespunzător (competent, prompt și cu viziune) în cadrul proceselor decizionale prin care se guvernează UE. Mai mult, chiar la nivelul Uniunii Europene, Comisia Europeană recomandă dezvoltarea capacității de evaluare și guvernare europeană, cele două concepte, „evaluare" și „guvernare" aflându-se într-o strânsă legătură.

În al treilea rând, o țară reflectă în esență tot un mod de organizare al oamenilor. În cazul organizării în limitele unei țări, oamenii au un bagaj de experiențe și aspirații comune (în funcție de țară, putem constata că la unii primează experiențele comune, iar la alții aspirațiile), într-un areal geografic. Din punct de vedere al caracteristicilor de organizare a unei țări, aceasta se aseamnă cu o organizație neguvernamentală nonprofit. Dacă putem privi o țară ca pe o organizație, de ce nu am putea evalua acea țară prin metodele prin care evaluăm o organizație?

EXPLICARE ȘI CORELARE A ELEMENTELOR CE POT FI INTRODUSE ÎN ANALIZĂ

Pentru a analiza organizațiile au fost dezvoltate diferite instrumente de evaluare, unele pornind din mediul de afaceri și fiind adaptate organizațiilor neguvernamentale, altele dezvoltate pentru a surprinde caracteristicile ONG-urilor și care ulterior au fost folosite și de companii. Elementele de bază ale analizei sunt însă aceleași, aplicabile direct sau după adaptare atât organizațiilor neguvernamentale nonprofit cât și companiilor.

Diferitele instrumente de evaluare organizațională, utilizate pentru strângerea datelor și analizarea acestora, lucrează pe aceleași componente ale vieții organizației, dar surprind aceste componente din perspective diferite. Instrumentele de evaluare organizațională sunt dezvoltate în special ca rezultat al cercetărilor efectuate de firme de consultanță în domeniul managementului, fie propuneri venite din mediul academic sau din partea unor fundații care oferă ele însele sprijin pentru dezvoltare în diverse domenii ale societății civile.

Pentru a putea face o analiză realistă unei organizații, trebuie cunoscut segmentul de piață în care activează aceasta. Evaluarea din perspectivă dinamică a unei organizații, adică din punct de vedere al dezvoltării acesteia, se sprijină pe câteva întrebări de bază: *unde își dorește să fie organizația?* (aspirații pe termen mediu și lung), *unde se găsește acum?* (situația de facto, ce are și pe ce se poate baza), *prin ce mijloace va ajunge de unde este unde își dorește să fie?* (strategie) și *ce știe să facă organizația?* (competențele și abilitățile organizației).

Răspunsurile la aceste întrebări, indiferent de perspectiva din care sunt date, trebuie să includă informații care corespund diferitor elemente din organizație.

Elementele de dezvoltare organizațională prezentate în capitolul următor se regăsesc în grilele de analiză pentru organizații neguvernamentale — instrument dezvoltat de către compania de consultanta McKinsey, și folosit cu succes

pentru îmbunătățirea structurală a organizațiilor de pe mai multe continente.

În ceea ce privește instrumentul de evaluare organizațională folosit, este util ca acesta să ofere o imagine - radiografie cât mai precisă a punctelor cheile, a acelor legături, cărora dacă li se aduc modificări, influențează și îmbunătățesc funcționarea întregului sistem.

ELEMENTE ȘI CONCEPTE CE POT FI PRELUATE ÎN EVALUAREA ORGANIZAȚIONALĂ A UNEI ȚĂRI

Aspirațiile: Misiune, viziune, țeluri

La nivelul unei organizații, misiunea bine exprimată și viziunea clară, cunoscute de membrii organizației, sunt elementele principale care duc la o bună planificare strategică și la o dezvoltare coerentă. Ele inspiră angajații, voluntarii și donatorii. Sunt baza strategiei și stabilesc prioritățile.

Conform cercetărilor efectuate în domeniu de către compania McKinsey, organizațiile care au avut cele mai semnificative rezultate ca impact social. au fost acelea care au abordat comprehensiv stabilirea misiunii, viziunii și a țelurilor organizației.

La nivelul unei țări, aspirațiile ar trebui să cuprindă locul și rolul pe care acea țară și le dorește față de cetățenii săi și pe care dorește să le aibă în exterior. Fără a ști exact încotro vrei să te îndrepți, orice drum e bun, iar evenimentele sunt trăite doar ca rezultate ale hazardului, ori ca influențe ale altor organizații (neguvernamentale, guvernamentale, statale, nonstatale, suprastatale), care au știut încotro vor să se îndrepte și au acționat în consecință.

În momentul de față, numeroase strategii și documente au ca scop intrarea României în NATO și aderarea la Uniunea Europeană. Acestea reprezintă într-adevăr obiective majore, care trebuie susținute de strategii naționale. Ele se referă însă la un orizont de timp mediu. Pe termen lung, la

nivelul unei țări, reprezintă obiective intermediare, și nu sunt suficiente pentru a reprezenta misiunea României în ansamblu.

Aspirațiile unei organizații, cuprinse în misiune, viziune și țeluri, oferă orientarea și coordonarea activității acelei organizații pe termen lung. Ele asigură continuitatea organizației, chiar dacă președintele fondator se retrage sau dacă se schimbă managerul.

Unul dintre obiectivele majore, intrarea României în NATO a fost atins. Alt obiectiv major este aderarea la UE. Care sunt însă aspirațiile pe termen lung ale României? Care va fi factorul de coeziune între strategiile naționale după ce România va fi acceptată ca membră a Uniunii Europene? Pentru ca politica României să nu mai fie reactivă, ci să fie coordonată printr-o atitudine proactivă, este necesară definirea interesului național pe termen lung, precum și acționarea în sensul atingerii acestui interes.

Factorii politici ar trebui să înțeleagă din perspectiva integrării europene și euro-atlantice că este necesară o viziune pe termen lung, 15 — 20 de ani, iar pentru continuitatea de implementare a viziunii pentru 2020 este necesar ca aceasta să fie definită prin dialog de către putere și opoziție.

Pentru a fi un membru valoros în oricare dintre echipe, și nu doar un instrument pentru implementarea politicii altora, orice organizație sau țară trebuie să aibă o viziune asupra propriului rol. Iar misiunea și viziunea sunt cu atât mai eficiente, cu cât sunt mai clare și asumate de către un număr mai mare de oameni și instituții.

Strategiile

Evaluarea strategiei include analizarea gradului în care programele de acțiune se subscriu strategiei. La nivelul unei țări, strategiile naționale urmăresc stabilirea unor obiective și coordonate (colaborări, responsabilități, etc.) pe termen mediu — lung. În cazul strategiilor naționale, trebuie pusă întrebarea dacă în cadrul lor sunt definite conceptele și obiectivele pe care le abordează, dacă sunt stabilite criterii

pentru îndeplinirea obiectivelor (calitativ și cantitativ) precum și ce sisteme de evaluare au fost incluse penru a verifica îndeplinirea obiectivelor propuse.

O organizație este cu atât mai eficientă în atingerea obiectivelor sale în conformitate cu aspirațiile sale, cu cât strategia este mai bine definită și programele dezvoltate sunt integrate acestei strategii. Astfel toate eforturile depuse pentru implementarea planurilor de acțiune cuprinse în programe, contribuie prin efectele lor la implementarea strategiei.

Un element important în implementarea diferitelor programe sunt și fondurile alocate acestora. În cazul României, pentru rezolvarea anumitor probleme sunt alocate și fonduri externe semnificative de la Uniunea Europeană precum și de la alți donatori sau finanțatori externi. Multe linii de finanțare sunt destinate exclusiv proiectelor organizațiilor neguvernamentale, acestea având un rol hotărâtor în crearea unei mase critice care, în contextul tranziției, să permită schimbarea pe diverse nivele și domenii ale societății.

Din perspectiva dezvoltării organizaționale, cuprind strategiile naționale roluri clare pentru toți factorii instituționali ce activează într-un domeniu? În domeniul securității naționale sunt stabilite în mod concret moduri și obiective ale cooperării între instituțiile statului cu responsabilități în domeniu, mediul academic și organizațiile neguvernamentale?

Pe anumite domenii strategiile naționale ale României prevăd implicarea tuturor factorilor ce activează într-un domeniu. Ar fi util să se studieze în ce măsură modelul de cooperarea instituțională dintr-un domeniu poate fi transpus într-un domeniu diferit.

Competențe și abilități ale organizației

Competențele și abilitățile organizaționale surprind ceea ce organizația, privită ca un ansamblu, știe să facă. Între competențe și strategii există o strânsă întrepătrundere. Strategiile influențează decizia de dezvoltare a anumitor competențe și abilități, iar competențele avute de către orga-

nizație influențează decizia de adoptare a uneia sau alteia dintre strategii.

McKinsey propune o evaluare care să cuprindă capacitățile organizației pentru *gestionarea performanței, planificarea la nivelul organizației, strângerea de fonduri, construirea și gestionarea relațiilor cu exteriorul, relațiile publice și marketingul, precum și influențarea politicilor publice.*

La nivelul unei țări, se poate face o împărțire care ține de competențe cu impact preponderent intern sau extern.

Pe plan intern, ar trebui evaluată capacitatea instituțiilor statului de a gestiona performanța și capacitatea de a planifica.

În România, *capacitatea de a gestiona performanța* este în dezvoltare, procesul de integrare în NATO și de aderare la UE catalizând și susținând efortul de a dezvolta standarde de performanță și sisteme care să măsoare performanța. Dacă în domeniul militar sau financiar criteriile de măsurare a performanței sunt clare și utilizarea continuă a unor standarde are tradiție, nu la fel stau lucrurile în alte domenii direct sau indirect legate de securitatea națională. În mod normal, un anumit număr de standarde ar trebui să existe în toate domeniile de activitate, fiind strâns legate de aspirațiile și strategiile adoptate, și să ofere repere anuale și pe termen lung. În mod cert este nevoie de timp pentru a dezvolta, implementa, evalua și îmbunătăți un sistem de măsurare a performanței, bazat pe un număr de indicatori cheie, incluzând impactul programelor și activităților din punct de vedere social, financiar, organizațional, etc. Este de asemenea foarte important procesul de feed-back asupra utilizării standardelor și a modului de măsurare a performanței. Dar în câte domenii de interes major se urmărește conștient obținerea feed-back-ului de la utilizatorii standardelor?

Capacitatea de planificare la nivel național, pentru a fi corectă și coerentă, trebuie să cuprindă toate domeniile de dezvoltare ale economiei și societății. Dacă nu există planificare corelată între sectoarele de activitate sau ale vieții

sociale, se va ajunge la situația în care obiectivele ambițioase și planurile de acțiune dintr-un domeniu nu pot fi puse în aplicare datorită slabei dezvoltări a capacității din alte domenii, unde nu există o planificare a dezoltării, sau unde aceasta nu este corelată cu obiectivele celorlalte domenii.

Evaluarea activității de planificare a unei țări ar trebui să cuprindă cel puțin capitolele pe care le cuprinde evaluarea făcută unei organizații (elemente de analiză propuse pentru organizații de McKinsey & Company): *monitorizarea mediului, planificarea strategică, planificarea financiară și bugetară, planificarea operațională și planificarea resurselor umane.*

Rolul planificării în fiecare dintre domeniile de activitate este evident, cu toate acestea trebuie atrasă atenția asupra faptului că, dacă există necorelări în momentul de față, acestea se vor mări cu timpul în condițiile în care nu sunt luate măsuri de redresare. Necorelări grave, cu posibile repercursiuni asupra securității naționale, se regăsesc și în domeniul resurselor umane, unde, fără planificare și susținere a obiectivelor stabilite, nu se obțin rezultate.

Pe plan extern, evaluarea poate cuprinde, la fel ca în cazul unei organizații, și la nivel de țară, capitolele de analiză a modului în care relațiile externe sunt construite și gestionate, a activității de relații publice și marketing, precum și a capacității de a influența politicile publice.

Relațiile publice și marketingul — se referă la locul pe care îl are o țară în comparație cu alte țări și percepția pe care o au alții asupra sa. În gestionarea relațiilor externe diplomația are un rol evident, dar nu poate acoperi în nici un caz întregul necesar de relații publice al unei țări. La dezvoltarea relațiilor publice dintre țări și la promovarea imaginii de țară poate contribui fiecare cetățean. Comportamentul românilor în străinătate contribuie pentru un cetățean al țării gazdă la conturarea imaginii pe care o are acesta despre România. Ținând cont de faptul că acesta poate influența pozitiv sau negativ imaginea pe care o are țara în exterior, ar putea fi dezvoltate programe care să amelioreze „exportul" de imagine pe care îl fac pe această cale cetățenii români (atât măsuri punitive pentru comportamente repro-

babile, cât și condiții pentru creșterea vizibilității în străinătate a unor români care pot fi ambasadori de imagine a țării, dar și programe adresate cetățenilor care călătoresc în străinătate). Comportamentul simplilor cetățeni români, când aceștia călătoresc în străinătate, poate din punct de vedere al imaginii propagate, intra în sfera interesului naționale. Aceasta o demonstrează și interesul lui Cristescu în acest sens, pentru că în 1941 elaborează „*Instrucțiuni cu privire la obligațiile românilor când merg în străinătate*", căci după trecerea granițelor țării „prima grijă este de a fi român" . Pentru a promova o imagine pozitivă/constructivă a unei țări prin proprii cetățeni, sunt necesare programe susținute și derulate pe mai mulți ani, fiind utilă cercetarea experiențelor altor țări în acest domeniu.

La nivelul simplu cetățean, la promovarea unei imaginii de țară contribuie și turiștii străini care vizitează România. Iar opinia pe care o au investitorii străini asupra României, poate avea deja un impact mai mare în țările lor de origine.

Un rol esențial în relațiile (publice) dintre țări îl au formatorii de opinie din țara cu care se dorește îmbunătățirea relațiilor publice. De exemplu, în evaluarea activității de relații publice a României ar trebui inclusă o analiză a programelor desfășurate de instuții românești special pentru jurnaliștii străini.

În ceea ce privește *marketing-ul unei țări*, se ține cont de faptul că privită din exterior, țara atrage atenția prin anumite elemente. Din această perspectivă și România trebuie să își găsească „nișa de piață". În cazul României este necesar ca elementele pozitive să fie promovate în mod conștient, ținând cont de aspirațiile și strategiile asumate la nivel național, precum și de ceea ce poate fi perceput ca realist și atractiv în exterior.

Exemplu recent de țară preocupată de marketing-ul său este Slovenia, care a considerat că nu este într-un grad suficient percepută ca identitate în plan extern. Pentru a schimba această situație, a demarat dezvoltarea unei strategii de imagine, pentru a dezvolta și implementa programe care să îi scoată în evidență unicitatea. (De la concurs de

design pentru un nou steag, până la căutarea și analiza unor slogane, de exemplu „Slovenia — țara de o oră" , pentru a sublinia faptul că în decursul unei ore poate fi vizitată de la nord la sud și de la est la vest).

O altă competență organizațională care se manifestă în exterior este *elaborării politicilor publice.*Transpusă *influențarea* la nivelul unei țări, domeniul supus evaluării este competența unei țări de a influența elaborarea politicilor externe care o vizează. Ținând cont de faptul că România se află în plin proces de pregătire a aderării la Uniunea Europeană, și că nici o instituție europeană nu poate oferi garanții asupra datei la care România va adera la Uniune, abilitatea de a influența politicile care vizează țara noastră, ar fi cu atât mai necesară. Aici este vorba de un rol proactiv față de fluxurile de informații și opinii care stau la baza formulării politicilor, dincolo de cifrele și datele concrete cuprinse în rapoartele de țară.

Un rol special în competența unei țări de a influența politicile care o vizează îl au serviciile de informații, care în urma analizării mediului extern, pot recomanda unde anume ar trebui intervenit informativ. Aceste intervenții pot include de la mijloacele specifice activității de informații la campanii de lobby, tot mai des utilizate și de țările vecine României. În afara operațiunilor punctuale, o țară ar trebui să desfășoare în mod continuu activități de influențare a politicilor care o vizează, mai ales într-un mediu competițional în care fiecare țară încearcă același lucru. Și nici o țară nu ar trebui să neglijeze faptul că bătăliile se poartă tot mai mult în plan informativ și imagistic.

În perioada societății informatice, activitățile ostile pota avea efecte dezastroase datorită propagării lor sistemice, și de asemenea, pot apare pe lângă vulnerabilități și oportunități unice. Serviciile de informații pot identifica din timp noile tendințe din mediul de securitate, la nivel international si impactul asupra țării pe termen scurt, mediu sau lung (acces la credite externe avantajoase, acces la resurse energetice, apă, poziționarea construcțiilor de infrastructură de către companii internaționale, conducte, șosele, rețele electrice.)

Starea de fapt a organizației

Starea de fapt a unei organizații este surprinsă în urma evaluăii unor elemente ca resursele umane, sistemele și infrastructura existente și structura organizatorică.

Un alt impelement de evaluare organizațională este și cultura organizatorică, care transpare pe mai multe nivele ale afirmării organizației, fiind cuprinsă și în starea de fapt, dar și la nivelul competențelor dezvoltate, a strategiilor sau a aspirațiilor. Și cultura organizațională poate fi inclusă în evaluarea unei țări, selectând doar elementele care au relevanță pentru dezvoltarea țării într-o anumită direcție.

Revenind la celelalte elemente prin care se caracterizează starea de fapt a unei țări, capitolul de evaluare a resurselor umane ar trebui adaptat pentru a anliza actorii de diferite dimensiuni și cu impact diferit în activitatea unei țări. Pe lângă evaluarea resurselor umane ca atare, din punct de vedere demografic, al pregătirii academice și profesionale, al stării de spirit, etc, trebuie luate în calcul instituțiile statului. Instituțiile statului pot fi, într-o primă etapă de evaluare asimilate funcțiilor dintr-o organizație, evaluarea lor trebuind să cuprindă însă mult mai multe elemente. Aici pot fi incluse și studiile efectuate pentru determinarea gradului de încredere pe care îl au cetățenii față de aceste instituții.

La nivel de țară, evaluarea interacțiunii dintre instituții se întrepătrunde cu analiza sistemelor instituționale și cea a structurii organizatorice.

În cazul României, unul din elementele nodale pentru îmbunătățirea funcționării instituționale este revizuirea proceselor prin care comunică instituțiile. Aici ar trebui analizate atât practica cât și procedurile existente în comunicarea verticală și orizontală, și aduse îmbunătăți care să eficientizeze procesul de comunicare și să îmbunătățească rezultatele acestuia. În plus trebuie analizat dacă există și cum funcționează procesul de feed-back pe instituții și probleme în discuție.

Alt element care poate contribui semnificativ la eficientizarea activității instituțiilor este o analiză din punct de vedere

al strucurii organizatorice, a „fișelor de post". În cazul în care într-o organizație responsabilitatea se regăsește în termeni nespecifici în fișele de post a mai multor angajați, ierarhizarea nu este clară în ceea ce privește responsabilitățile și răspunderea, este posibil ca anumite probleme să nu fie soluționate în timp util și în parametrii optimi. Doar observând practica, putem trage concluzia că se regăsesc situații similare și la nivelul unei țări, pornind de la „fișele de post" ale instituțiilor, atât cele centrale, cât și la nivel local, la serviciile descentralizate.

Pentru a evalua funcționarea sistemelor instituționale se pot identifica numeroase instrumente și elemente de anliză. De mare utilitate în cazul României ar fi ca tipurile de evaluări care se fac sistemelor instituționale din anumite segmente de activitate să fie utilizate ca model și în alte segmente, și ca rezultatele analizei să nu rămână doar „concluzii" ale unui raport, ci să ofere datele de pornire pentru îmbunătățiri viitoare.

CONCLUZII

Studiul și-a propus să atragă atenția asupra potențialului pe care îl are evaluarea organizațională aplicată unei țări. Evaluarea organizațională urmărește acele elemente care fac instituția sau compania respectivă să fie mai eficientă.

De ce nu s-ar putea urmări aceleași elemente și pentru sporirea competitivității unei țări, ținând cont că și o țară evoluează într-un mediu concurențial? Prin abordarea organizațională pot fi evaluate și aduse îmbunătățiri pe domenii specifice. Ar fi însă de mare utilitate, ca aceste evaluări sectoriale să se înscrie într-un cadru mai larg, pornind de la aspirațiile de dezvoltare la nivel național.

Pentru evaluarea organizațională a unor sectoare de activitate și chiar a țării în ansamblu, pot fi folosite diferite instrumente de evaluare, cele mai utile fiind acelea care cuprind detaliat elementele asupra cărora ar trebui intervenit ulterior pentru a îmbunătăți organizația.

Apar ca evidente necesitatea de a dezvolta ca țară un demers coerent, strategic și continuu de dezvoltare și includere a politicilor și strategiilor naționale pe termen lung în obișnuința modului de lucru curent. Baza unor asemenea strategii trebuie să fie evaluări cât mai concentrate, care să surprindă elementele cheie care pot influența în bine funcționarea sistemului.

Pentru dezvoltarea acestui tip de evaluare ca parte a ciclului de dezvoltare, instituțiile guvernamentale Române ar putea folosi exemplele de bună practică existente pe tematica evaluării în anumite domenii ale sectorului privat, fie economic, fie nonprofit. Este necesar să se treacă de la paradigma politică la paradigma strategică.

România are de recuperat decalaje de decenii pentru a junge la un nivel mediu de dezvoltare în cadrul Uniunii Europene. Este nevoie de aproximativ 30–50 de ani pentru a recupera aceste decalaje prin mijloace clasice. Oare nu există alte mijloace pentru a reduce cât mai mult posibil aceste diferențe? Tema lucrării, propunerea de a evalua și îmbunătăți organizațional România, este o încercare în acest sens.

BIBLIOGRAFIE

Strategia de Securitate Națională a României, București 2001

Reinventing Government — Gore Commission, SUA, 1993

Drăgan G, *Politica de coeziune economică și socială a Uniunii Europene*, ASE, 2004

Handy Ch, *Understanding Organizations*, Penguin Business Management, ediția a 4-a, England, 1993

Kotler Ph / Roberto E, *Social Marketing*, ECON Verlag, Düsseldorf, 1991

McKinsey & Company, *Effective Capacity Building for Nonprofit Organizatios*, realizat pentru Venture Philantropy Partners, 2001 www.europa.eu.int

www.ince.ro

www.mapn.ro

În colecția
STUDII DE SECURITATE
au apărut:

- *Serviciile de informații și decizia politică*, Mireille Rădoi
- *Law & Crime. Net*, Ilie Botoș, Monica Șerbănescu și Dumitru Zamfir
- *Armata și societatea în tranziție*, Marian Zulean
- *Securitatea internațională și Forțele Armate*, Jean Calaghan și Franz Kearnic

vor apărea:

- *Balanță și hegemonie. România în politica internațională până în 1989*
- *Managementul riscurilor politico-militare*, Ionel Lanciu și Monica Șerbănescu

În colecția
SENS
au apărut:

- *Măștile efemerului*, Denis Tillinac
- *Națiunea și provocările postmodernității*, Dan Dungaciu
- *Războaiele cu arabii*, Alexis de Tocqueville

vor apărea:

- *Națiune și naționalism în era globalizării*, Anthony Smith
- *Aromâni, vlahi, meglenoromâni în Europa de sud-est*, Thede Kahl

În colecția
COMUNICARE/MEDIA
au apărut:

- *Istoria presei române* (antologie), Marian Petcu
- *Bătălia pentru știri*, Michael Palmer
- *Comunicarea interpersonală*, Irena Chiru
- *Jurnaliștii – vedete, scribi sau conțopiști*, Michael Palmer și Denis Ruellan
- *Comunicare, semiotică și semne publicitare*, Jean Jacques Boutaud
- *Jurnalism radio*, Vasile Traciuc
- *Comunicare, televiziune, democrație*, Patrick Lecomte
- *Psihologia reclamei*, Dimitrie Todoran
- *Management în cinematografie*, Lucian Pricop
- *Analiza discursului. Ipoteze și ipostaze*, Daniela Roventa-Frumușani
- *Mesajul subliminal în comunicarea actuală*, Doina Ruști
- *Televizorul în micul infern*, Zoltan Rostas și Sorin Stoica coord.

vor apărea:

- *Relațiile publice – abordare interdisciplinară*, Adela Rogojinaru
- *Comunicarea managerială*, Stephane Olivesi
- *Radiodifuziunea română: de la înființare la etatizare*, Filaret Acatrinei
- *Media și Terorismul*, Isabelle Garcin-Marrou

În seria
CATEDRA
au apărut:

- *Manual de fotojurnalism*, Gabriela Sandu
- *Manual de jurnalism* (vol. I și II), Cristian Florin Popescu
- *Presa cotidiană*, Maurice Mouillaud și Jean-Francois Tetu
- *O istorie ilustrată a publicității*, Marian Petcu
- *Introducere în teoria comunicării*, Valentina Marinescu
- *Dicționarul jurnalistului de radio*, Radu Bîlbîie
- *Comunicarea nonverbală în spațiul public*, Septimiu Chelcea coord.

va apărea:

- *Dicționar de televiziune*, Lucian Ionică

În seria
PUBLICIȘTI ȘI PUBLICAȚII
vor apărea:

- *Caragiale – publicist*, Adriana Ghițoi
- *Tânărul scriitor – o monografie*, Răduț Bâlbâie
- *Nicolae Iorga*, Pamfil Șeicaru
- *București anului '35*, selecție de articole din revista *Realitatea Ilustrată*
- *Nae Ionescu publicist*, Romina Surugiu

În colecția
SOCIOLOGIE
au apărut:

- *Sociologie aplicată*, Carmen Bălan
- *Ingrup vs. Outgrup în imaginarul biblic*, Ana-Maria Bărbulescu
- *Meșterii țărani români*, Paul H. Stahl și Marin Constantin
- *Recunoașterea internațională a Școlii Gusti*, Valentina Pricopie
- *Societate și arhitectură. O perspectivă sociologică*, Trăilă Cernescu
- *Evaluarea politicilor publice*, Mireille Rădoi
- *Cercetarea monografică a familiei*, Xenia Costaforu
- *Schimbarea în organizația militară*, Claudiu Nicolae

vor apărea:

- *Sociologie politică: de la regim politic, la globalizare*, Mihai Milca
- *Politică și sociologie în România comunistă*, Dan Dungaciu
- *Tradiția și rolul ei social. Factorul ideal – studii*, Eugeniu Sperantia

CARTEA PRIN POȘTĂ
Pentru cărțile comandate, editura suportă costurile de transport prin poștă. În plus:
– pentru **2** cărți se acordă o reducere de 10 %
– de la **3** cărți în sus se acordă o reducere de 15%.
Pentru a obține oricare dintre aceste cărți, trimiteți comanda dumneavoastră pe adresa: **Editura TRITONIC, C.P. 3-12 BUCUREȘTI,** prin fax: **021.242.54.09,** la tel.: **0788.360.391** sau prin e-mail la: **tritonic@fx.ro; editura@tritonic.ro**.

Cristian Troncotă (n. 1954) este prof. univ. dr. şi decan la Academia Naţională de Informaţii. Asiduu cercetător în arhivele secrete, renumit specialist în analiza evoluţiei organizaţiilor de intelligence din România, dar şi din alte ţări.

"Reprezintă democraţia, într-o perioadă de tranziţie prelungită, o valoare pentru securitatea naţională? Va reuşi noul concept de securitate prin cooperare să aducă pacea globală? Este nevoie de un sistem educaţional pentru securitate în rândul tineretului? Respectarea standardelor de calitate a produselor, din orice domeniu, are legătură cu securitatea naţională? Care sunt standardele internaţionale şi cât am reuşit să le adaptăm pe plan naţional în domeniul protejării datelor, documentelor şi informaţiilor secrete? Dar în domeniul securităţii alimentelor? Avem noi românii şi ceva pozitiv în tradiţia activităţii de informaţii care poate fi folositor actualului proces de restructurare instituţională? Cum se respectă drepturile şi libertăţile fundamentale în activitatea de informaţii? Iată câteva dintre întrebările formulate, dar şi o mai mare varietate de răspunsuri posibile, care toate la un loc dovedesc ţinută şi rigoare academică, precum şi o reală responsabilitate civică din partea celor care s-au încumetat să-şi dezvăluie neliniştile în paginile acestui volum."

Cristian Troncotă

STUDII DE SECURITATE
TRITONIC

www.studiidesecuritate.ro
www.tritonic.ro

ISBN 973-733-009-9